1/2006

Datenschutz Nachrichten

29. Jahrgang
ISSN 0137-7767
9,00 Euro



Datenschutz in Europa

European Data Protection Supervisor ■ Artikel 29-Gruppe ■ Europäische Datenschutzorganisationen ■ Polizeilicher Datenaustausch in der EU ■ Vorratsdatenspeicherung ■ Volkszählung 2010 ■ Datenschutznachrichten ■ Technik ■ Gentechnik ■ Rechtsprechung ■ Buchbesprechungen ■ Pressemitteilungen

Deutsche Vereinigung für Datenschutz e.V.
www.datenschutzverein.de

Autoren dieser Ausgabe

Dr. Patrick Breyer

Jurist, Meldorf
P.Breyer@daten-speicherung.de

Peter J. Hustinx

European Data Protection Supervisor, Brussels
phustinx@edps.eu.int

Peter Schaar

Dipl.-Volkswirt, Bonn
Bundesbeauftragter für den Datenschutz und die Informationsfreiheit
Vorsitzender der Artikel 29-Gruppe
Peter.schaar@bfdi.bund.de

Karin Schuler

Dipl.-Informatikerin, Bonn
Mitglied des Vorstandes der Deutschen Vereinigung für Datenschutz
schuler@datenschutzverein.de

Dr. Thilo Weichert

Leiter des Unabhängigen Landeszentrums für Datenschutz
Schleswig-Holstein, Kiel
weichert@datenschutzzentrum.de

Termine

09.04.2006
DVD-Vorstandssitzung in Berlin*

07.05.2006
Redaktionsschluss DANA 2/2006
Vorratsdatenspeicherung

08.06.2006
Datenschutzfachtagung der BTQ Niedersachsen in Hannover (www.btq.de)

02.07.2006
DVD-Vorstandssitzung in Bonn*

07.08.2006
Redaktionsschluss DANA 3/2006
Arbeitnehmer-Datenschutz

15.08.2006
BigBrotherAwards Nominierungsschluss

20.10.2006
BigBrotherAwards-Verleihung in Bielefeld

28.10.2006
DVD-Vorstandssitzung in Bonn*

29.10.2006
DVD-Mitgliederversammlung in Bonn

07.11.2006
Redaktionsschluss DANA 4/2006
Big Brother Awards 2005

15.-17.11.2006
25. RDV / 30. Dafta in Köln

* interessierte DVD-Mitglieder können gerne teilnehmen, bitte in der Geschäftsstelle melden

DANA
Datenschutz Nachrichten
ISSN 0137-7767
29. Jahrgang, Heft 1

Herausgeber
Deutsche Vereinigung für Datenschutz e.V. (DVD)
DVD-Geschäftsstelle:
Bonner Talweg 33-35, 53113 Bonn
Tel. 0228-222498
E-Mail: dvd@datenschutzverein.de
www.datenschutzverein.de

Redaktion (ViSdP)
Rainer Scholl
c/o Deutsche Vereinigung für Datenschutz e.V. (DVD)
Bonner Talweg 33-35, 53113 Bonn
dana@datenschutzverein.de
Den Inhalt namentlich gekennzeichneter Artikel verantworten die jeweiligen Autoren.

Druck
Wienands Printmedien GmbH
Linzer Str. 140, 53604 Bad Honnef
wienandsprintmedien@t-online.de
Tel. 02224 989878-0
Fax 02224 989878-8

Bezugspreis
Einzelheft 9 Euro. Jahresabonnement 32 Euro (incl. Porto) für vier Hefte im Jahr. Für DVD-Mitglieder ist der Bezug kostenlos.
Ältere Ausgaben der DANA können teilweise noch in der Geschäftsstelle der DVD bestellt werden.

Leserbriefe
Leserbriefe sind erwünscht, deren Publikation sowie eventuelle Kürzungen bleiben vorbehalten.

Abbildungen
Titelbild u. Rückseite:
Frans Jozef Valenta

Europäische Dimensionen

Die für Deutschland maßgebliche Politik wird heute – oft mit fragwürdiger demokratischer Legitimation unter Umgehung der Parlamente – in »Brüssel« gemacht. In den letzen Jahren war das unter dem Vorwand der Terrorbekämpfung eher eine Politik gegen die Persönlichkeitsrechte der Menschen.
Die Globalisierung und die wachsende Bedeutung des eCommerce führen gleichzeitig zu einer Internationalisierung der Datenverarbeitung mit weltweitem Austausch personenbezogener Daten. Für die Betroffenen ist dabei kaum noch transparent, was mit ihren Daten geschieht, wo sie wie und wozu verarbeitet und genutzt werden.
Den europäischen Institutionen käme nicht nur die Aufgabe zu, ein hohes Schutzniveau der Datenverarbeitung über die nationalen Grenzen hinweg in einem vereinten Europa sicher zu stellen. Sie könnten auch als Anwalt für die Rechte der Menschen in Europa und als Verhandlungspartner der außeuropäischen Nationen die Globalisierung der Datenverarbeitung begleiten. Aber z.B. die Auseinandersetzung um die Flugdaten hat gezeigt, dass die Kräfte sehr stark sind, die die Rechte der Menschen den internationalen Wirtschaftsinteressen und den ausufernden Überwachungsbedürfnissen der Regierungen opfern wollen.
Deshalb wird es um so wichtiger, den Datenschutz in seiner europäischen Dimension zu sehen; mit dieser Ausgabe der Dana wollen wir einen Beitrag dazu leisten.

Rainer Scholl

Inhalt

Peter J. Hustinx

The European Data Protection Supervisor after two years

European institutions such as the European Commission, the European Parliament and the Council are playing an important role in setting common data protection standards for 25 EU member states. Since a few years, such standards also apply at EU level, with independent supervision by a European Data Protection Supervisor. After two years, the EDPS gives a ›birds-eye view‹ of his activities.[1]

Legal framework

Article 286 of the EC Treaty, adopted in 1997 as part of the Treaty of Amsterdam, provides that Community acts on the protection of individuals with regard to the processing of personal data and the free movement of such data should also apply to the Community institutions and bodies, and that an independent supervisory authority should be established.

These Community acts are Directive 95/46/EC, which lays down a general framework for data protection law in the member states, and Directive 97/66/EC, a sector specific directive which has been replaced by Directive 2002/58/EC on privacy and electronic communications. Both directives aimed at a high level of protection and a free flow of personal data in the EU. In the early 1990's, the Commission stated that Community institutions and bodies should be bound by similar legal safeguards, enabling them to take part in this free flow of data, subject to equivalent rules of protection. However, until the Treaty of Amsterdam, a legal basis for this was lacking.

The rules referred to in Article 286 EC Treaty have been laid down in Regulation (EC) No. 45/2001 of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data[2], which entered into force in 2001. This Regulation has also provided for an independent supervisory authority, referred to as ›European Data Protection Supervisor‹, with a number of tasks and powers.

The Regulation applies to the »processing of personal data by Community institutions and bodies insofar as such processing is carried out in the exercise of activities all or part of which are within the scope of Community law«. This means that only activities which are totally outside the ›first pillar‹ framework – e.g. police or judicial cooperation in criminal matters – are not subject to the supervisory tasks and powers of the EDPS. Community institutions apart from those already mentioned, include the Court of Justice, except in its judicial function. The term ›Community bodies‹ refers to other entities, such as a growing number of agencies, established in various EU member states.

The definitions and the substance of the Regulation closely follow the approach of Directive 95/46/EC. One could say that Regulation 45/2001 is the implementation of that Directive at European level. This means that the Regulation deals with general principles such as fair and lawful processing, proportionality and compatible use, special categories of sensitive data, information to be given to the data subject, rights of the data subject, obligations of controllers, and with supervision, enforcement and remedies. A separate chapter deals with the protection of personal data and privacy in the context of internal networks. This chapter is the implementation at EU level of ›old‹ Directive 97/66/EC on privacy and communications.

An interesting feature of the Regulation is the obligation for Community institutions and bodies to appoint at least one person as Data Protection Officer. These officers have the task of ensuring the internal application of the provisions of the Regulation, including the notification of processing operations, in an independent manner. All Community institutions and a few bodies now have these officers, and some of them have been active for a number of years. This means that important work has been done to implement the Regulation, even before the EDPS and Assistant EDPS were appointed in January 2004. DPOs have the duty to cooperate with the EDPS, and thus provide a very important and much appreciated network.

Task and powers of EDPS

The tasks and powers of the EDPS are described in Articles 41, 46 and 47 of the Regulation. Article 41 lays down the general mission of the EDPS – to ensure that the fundamental rights and freedoms of natural persons, and in particular their privacy, with regard to the processing of personal data are respected by Community institutions and bodies – and sets out some specific elements of this mission. These general responsibilities are developed and specified in Article 46 and 47 with a detailed list of duties and powers.

This presentation of responsibilities, duties and powers follows in essence the same pattern as those for national supervisory bodies: i.e. hearing and investigating complaints, conducting other inquiries, informing controllers and data subjects, carrying out prior checks when processing operations present specific risks, etc. The Regulation gives the EDPS the power to obtain access to relevant information and relevant premises, where this is necessary for inquiries. He can also impose sanctions and refer a case to the Court of Justice.

Some tasks have a more special character. The task of advising the Com-

[1] More information will be available in Annual Report 2005 as from April 2006.

[2] OJ L 8, 12.1.2001, p. 1.

mission and other Community institutions about new legislation – emphasized in Article 28 (2) by an obligation for the Commission to consult the EDPS when it adopts a legislative proposal relating to the protection of personal data – also relates to draft Directives and other measures that are designed to apply at national level, or to be implemented in national law. This task allows the EDPS to have a look at privacy implications at an early stage and to discuss any possible alternatives, regardless of the ›pillar‹ involved. Monitoring relevant developments which may have an impact on the protection of personal data is also an important task.

The duty to cooperate with national supervisory authorities and supervisory bodies in the ›third pillar‹, such as the supervisory bodies for Schengen, Europol and Eurojust, has a similar character. As a member of the Article 29 Working Party, set up to advise the Commission and to develop harmonised policies, the EDPS has the opportunity to contribute at that level. Cooperation with supervisory bodies in the ›third pillar‹ allows him to observe developments in that context and to contribute to a more coherent and consistent framework for the protection of personal data, regardless of the ›pillar‹ or specific context involved.

These tasks and powers allow a distinction in three main roles. These roles have been taken as starting points for the new authority and will continue to serve as guidelines in the near future:

- a supervisory role, to monitor and ensure that Community institutions and bodies comply with applicable legal safeguards whenever they process personal data;
- a consultative role, to advise Community institutions and bodies on all relevant matters, and especially on proposals for legislation that have an impact on the protection of personal data;
- a cooperative role, to work with national supervisory authorities and supervisory bodies in the ›third pillar‹ of the EU, with a view to improving consistency in the protection of personal data.

During the first two years, important progress has been made in these three areas. It has been stated repeatedly that more and more EU policies depend on the lawful processing of personal data. Many public or private activities in a modern society nowadays generate personal data or use such data as input, and this is not different for EU institutions and bodies. This means that effective protection of personal data, as fundamental value underlying EU policies, should be seen as a condition for their success. This message has been received well and will continue to drive activities in the near future.

Supervision

A first emphasis has been put on the development of the network of Data Protection Officers. In November 2005, a position paper[3] was issued on the role of DPOs in ensuring effective compliance with Regulation 45/2001. The position paper was sent to the heads of the EU administration and underlined the role of the DPO as a strategic partner for institutions and bodies in ensuring compliance. One of the key messages was that all bodies need to appoint a DPO as a vital first step on their way towards compliance.

A major second emphasis has been on the prior checking of processing operations which are likely to present specific risks for data subjects, as mentioned in Article 27 of the Regulation. Although this task was typically designed to deal with new processing operations, most prior checks have been ›ex post‹ prior checks, due to the fact that many existing systems would have qualified for prior checking, had the EDPS been available at the time of their entering into operation. In 2005, 34 opinions were issued in prior checking cases, 30 of which were on existing systems of various institutions and bodies. In most cases, opinions recommended substantial improvements to ensure full compliance. Opinions are published at the EDPS website and their follow up is monitored. At the end of 2005, 29 notifications were in process and many more are expected in the near future. Institutions and bodies have been encouraged to submit their notifications for prior checking not later than by spring 2007.

A third emphasis has been on the handling of complaints. However in 2005, only 5 out of 27 complaints received by the EDPS were declared admissible and further examined. In practice, a large majority of complaints, such as complaints about national data protection, do not raise issues for which the EDPS is competent. In such cases, the complainant is informed in a general way and, if possible, advised on a more appropriate alternative. With respect to the handling of complaints within his competence, the EDPS is in contact with the European Ombudsman to examine a potential scope for collaboration in the near future.

Considerable efforts have also been invested in the elaboration of a background paper on public access to documents and data protection, issued in July 2005 with a view to promote a balanced approach to both fundamental interests. Special attention has also been given to supervision of EURODAC which requires a close cooperation with supervisory authorities in the member states.

Consultation

A first priority in this area has been the definition of a policy on the role of the EDPS as an advisor to the Community institutions on proposals for legislation and related documents. A policy paper was issued in March 2005, which emphasizes that the advisory task has a wide scope and deals with all proposals for legislation with an impact on the protection of personal data. The policy paper also sets out the substantive approach which the EDPS intends to take to such proposals for legislation, as well as his procedural role in the different stages of the legislative process. The European Commission is making good use of the availability of the EDPS to make informal comments on a draft proposal before it is submitted for consultation. A formal opinion is always published, often presented in a committee of the Parliament, or the competent working party of the Council, and systematically followed on its way through the legislative process.

The EDPS issued six formal opinions in 2005 which reflect the relevant subjects on the policy agenda of the Commission, the Parliament and the Council. Important opinions related to the exchange of personal data in the third pillar, the development of EU wide information systems – a Visa Information System (VIS) and a second generation Schengen Information System (SIS II) – and the highly controversial subject of the retention of traffic data on electronic communications for access by law enforcement authorities.

[3] With other publications mentioned in this article, available at www.edps.eu.int (›EDPS website‹).

The EDPS has also, for the first time, made use of the possibility to intervene in cases before the Court of Justice which raise important questions of data protection. The Court granted a request of the EDPS to intervene in two cases before the Court on the transfer of PNR-data on airline passengers to the United States, in support of the conclusions of the Parliament. The EDPS presented both written and oral observations, and is now looking forward to a decision of the Court.

The EDPS also exercised his advisory role with respect to administrative measures, and more in particular on implementing rules of institutions and bodies in the area of data protection. This provides an opportunity to influence, in a more structural fashion, the way in which data protection policies are implemented. In this context, the EDPS has developed an approach to the specific implementing rules concerning the role of DPOs.

The EDPS has a special task in monitoring new developments that have an impact on the protection of personal data. He has therefore made an initial evaluation of important new technological advances, and developments in policy and legislation that will be followed systematically in 2006 and thereafter.

Cooperation

An important platform for cooperation with national supervisory authorities is the Article 29 Working Party, set up by Article 29 of Directive 95/46/EC and presently chaired by Peter Schaar, of which the EDPS is a full member. Some important proposals for legislation were covered by the EDPS and the Working Party in separate opinions. In these cases, the EDPS has welcomed the general support of national colleagues as well as additional comments which can lead to better data protection. The EDPS has also invested in the development of common positions which can contribute to more consistency in data protection law in the European Union.

Cooperation with supervisory bodies in the ›third pillar‹ has concentrated to a large extent on the preparation of common positions with a view to the development of a highly needed framework for data protection in the ›third pillar‹, dealing with police and judicial cooperation in criminal matters. More specifically, discussions have taken place about a new system of supervision with regard to SIS II, which will build on a close cooperation between national supervisory authorities and the EDPS.

The EDPS has cooperated actively in the wider context of the European and International Conferences of Data Protection Commissioners. In September 2005, in cooperation with Council of Europe and OECD, the EDPS hosted a workshop on data protection in international organisations.

Communication

The EDPS has also invested in development of an information strategy and enhancement of information and communication tools. An information campaign for EU institutions and bodies and all Member States, with brochures in all Community languages, was followed by the introduction of a press service and a regular newsletter, and will soon be completed by the introduction of a new website, as the most important tool of communication. Meanwhile the EDPS has continued to provide useful information, both in response to specific requests, and in opinions, papers and speeches at the present website.

Resources

Major attention has been given to the development of human resources. Important results have been reached, both in recruitment and in special programs for stages and secondment of national experts. A combination of means has resulted in additional flexibility and continuous challenges for staff. The size of the organisation in 2006 will be slightly higher than 25 full time positions.

The EDPS is satisfied that the budget authorities have provided the budgetary means for consolidation and limited growth of the organisation, with due respect for urgent tasks in supervision and consultation on data protection in most institutions and bodies.

Finally, it is difficult to overstate the importance of the administrative agreement, concluded in 2004 with the Commission, the Parliament and the Council, which has enabled the EDPS to benefit from outside support where appropriate, and to invest most resources in primary activities.

Conclusion

The EDPS has started in January 2004, but most of the first year was used to make the first steps in the ›building of a new institution‹ and the development of its strategic roles at Community level, to monitor and ensure the application of legal safeguards for the protection of personal data. Most staff joined the EDPS only at the end of 2004.

After two years, the independent authority is shaping up well, and it has also been able to position itself as a new authoritative and visible player in a highly relevant area. This is partly due to many persons in different institutions and bodies with whom we closely cooperate and who are responsible for the way in which data protection is ›delivered‹ in practice, but most of all to the members of the staff who take part in the mission of the EDPS and who continue to make a major difference in its results.

Peter Schaar

Die Kooperation der Datenschutzaufsichtsbehörden am Beispiel der Artikel 29-Gruppe

Die Artikel 29-Gruppe ist eines der wichtigsten internationalen Kooperationsgremien auf dem Gebiet des Datenschutzes. Ihr Hauptziel besteht darin, innerhalb der EU ein einheitlich hohes Datenschutzniveau zu gewährleisten.

Datenschutz ist heute mehr denn je ein internationales Thema, denn technologische Entwicklungen, elektronische Dienste und globale Projekte lassen sich durch noch so gute nationale Regelungsansätze nicht mehr angemessen steuern. Die Entstehung einer globalen Informationsgesellschaft bringt große technische, rechtliche, soziale und wirtschaftliche Veränderungen und damit eine intensive Verarbeitung und einen weltweiten Austausch personenbezogener Daten mit sich. Den damit verbundenen Herausforderungen für den Schutz der Persönlichkeitsrechte kann nur durch die internationale Kooperation auf dem Felde des Datenschutzes effektiv begegnet werden, zumal die Datenverarbeiter – seien es öffentliche oder nicht-öffentliche Stellen – zunehmend europaweit, international, ja global agieren.

Die Europäische Datenschutzrichtlinie (RL 95/46/EG vom 24.10.1995) hat nicht nur in den Mitgliedstaaten der EU einen Harmonisierungsschub des Datenschutzrechts ausgelöst; sie hat vielmehr weltweit die Datenschutzdiskussion gefördert und dazu beigetragen, dass nunmehr viele – auch außereuropäische – Staaten Datenschutzgesetze erlassen haben oder vorbereiten. Der Datenschutz in der EU hat ein festeres Fundament in der Grundrechtecharta vom 7.12.2000 bekommen. In Artikel 8 ist der Schutz der personenbezogenen Daten als Grundrecht jeder Person verankert. Die Überwachung der Rechtsbefolgung durch unabhängige Datenschutzkontrollstellen ist integraler Bestandteil dieses Rechts. Durch die Aufnahme des Datenschutzes in den Vertrag über eine Verfassung für Europa, in dem die Charta als integraler Bestandteil enthalten ist, wird die Grundlage für den Datenschutz noch weiter verbessert. In Artikel I-51 soll jedem Menschen das Recht auf Schutz der ihn betreffenden personenbezogenen Daten zugestanden werden. Außerdem soll danach die Befolgung der Datenschutzvorschriften von einer unabhängigen Behörde überwacht werden.

Gleichermaßen bedeutsam ist die verstärkte Zusammenarbeit der nationalen Datenschutzbehörden. Die »Gruppe für den Schutz von Personen bei der Verarbeitung personenbezogener Daten (Artikel 29-Gruppe)« wurde gemäß Artikel 29 der Datenschutzrichtlinie im Jahr 1996 eingerichtet. Neben den Datenschutzbeauftragten der Mitgliedstaaten der EU gehört der Europäische Datenschutzbeauftragte der Artikel 29-Gruppe an. Zudem nimmt die Europäische Kommission – allerdings ohne Stimmrecht – an den Sitzungen teil. Ein herausragendes Ereignis der letzten Jahre war die Aufnahme zehn neuer Mitgliedstaaten zum 01.05.2004. Vorher hatten die neuen Mitglieder bereits die Möglichkeit, als Beobachter an den Sitzungen teilzunehmen.

Die Beiträge der Gruppe in Form von (inzwischen 116) Arbeitspapieren, Stellungnahmen oder Empfehlungen orientieren sich an dem Ziel, ein europaweit hohes Datenschutzniveau zu gewährleisten und dabei auch die Rechte derjenigen Personen zu schützen, deren Daten aus der EU in Drittstaaten übermittelt werden. (europa.eu.int/comm/justice_home/fsj/privacy/workinggroup/wpdocs/2005_de.htm)

Aufgaben der Artikel 29-Gruppe

Artikel 29 der allgemeinen Datenschutzrichtlinie setzte die Gruppe als unabhängiges Beratungsgremium ein und knüpfte ihre Tätigkeit im Wesentlichen an die Aufgaben der Kommission. Die Tätigkeit der Gruppe ergibt sich aus den Aufgaben und Funktionen, die in Artikel 30 der Richtlinie aufgeführt sind:

- Fragen im Zusammenhang mit den zur Umsetzung dieser Richtlinie erlassenen einzelstaatlichen Vorschriften zu prüfen, um zu einer einheitlichen Anwendung beizutragen.
- Zum Schutzniveau in der Gemeinschaft und in Drittländern gegenüber der Kommission Stellung zu nehmen.
- Die Kommission bei geplanten Änderungen dieser Richtlinie, bei Entwürfen zusätzlicher oder spezifischer Maßnahmen zur Wahrung der Rechte und Freiheiten natürlicher Personen bei der Verarbeitung personenbezogener Daten sowie bei allen anderen Entwürfen von Gemeinschaftsmaßnahmen zu beraten, die sich auf diese Rechte und Freiheiten auswirken.
- Stellungnahmen zu den auf Gemeinschaftsebene erarbeiteten Verhaltensregeln abzugeben; die Kommission zu informieren, wenn sich im Bereich des Schutzes von Personen bei der Verarbeitung personenbezogener Daten zwischen den Rechtsvorschriften oder der Praxis der Mitgliedstaaten Unterschiede ergeben, die die Gleichwertigkeit des Schutzes in der Gemeinschaft beeinträchtigen könnten.
- Von sich aus Empfehlungen zu allen Fragen abzugeben, die den Schutz von Personen bei der Verarbeitung personenbezogener Daten in der Gemeinschaft betreffen.

Harmonisierte Datenschutzpraxis

In ihrem Bericht zur Umsetzung der Datenschutzrichtlinie (Erster Bericht über die Durchführung der Datenschutzrichtlinie (95/46/EG) vom 15.05.2003 (KOM (2003) 265 endg.) hat die Kommission verdeutlicht, dass erhebliche Defizite bei der Umsetzung

der Richtlinie bestehen. Im Mittelpunkt der Arbeit der Artikel 29-Gruppe steht deshalb die Schaffung einer weiter harmonisierten Rechtslage und Datenschutzpraxis in den Mitgliedstaaten.

Die Gruppe hat mit einem auf lange Sicht angelegten Programm mit einer Bestandsaufnahme der Rechtsdurchsetzung in den Mitgliedstaaten begonnen. (WP 101).

Einer verbesserten Zusammenarbeit zwischen den Datenschutzkontrollstellen dienen auch

- ein zweimal jährlich stattfindender Workshop zur Beschwerdebearbeitung und ein Intranet für den Informationsaustausch und die Behandlung länderübergreifender Fälle,
- der regelmäßige informelle elektronische Informationsaustausch zwischen den einzelnen Datenschutzkontrollstellen in Form von Fragen und Antworten zum Recht und zur Rechtspraxis in allen Mitgliedstaaten,
- die Festlegung einer vereinfachten Bearbeitungsstruktur von verbindlichen Unternehmensregelungen (WP 107, 108) und
- die Vereinfachung der Meldepflichten über die Verarbeitung personenbezogener Daten für Unternehmen, die in mehreren Mitgliedstaaten niedergelassen sind (WP 106).

Institutionelle Zusammenarbeit

Die Beziehungen zwischen der Artikel 29-Gruppe und dem Europäischen Parlament (EP) sind gerade im Hinblick auf den Grundrechtsschutz von entscheidender Bedeutung. Deshalb ist es erfreulich, dass sich die Zusammenarbeit vertieft hat. So hat das Parlament die meisten Stellungnahmen der Gruppe in seinen Entschließungen zu Datenschutzfragen mit einbezogen, etwa bei der Diskussion über die Vorratsspeicherung von Telekommunikationsdaten oder bei den Vorgaben für biometrische Reisepässe. Insbesondere zu dem Ausschuss für Freiheitsrechte des EP bestehen sehr enge Kontakte. Ich bin optimistisch, dass die Zusammenarbeit noch weiter ausgebaut wird, da das Parlament die Auffassungen und Belange aller europäischen Bürger vertritt und stets nachhaltig für den Schutz und die Weiterentwicklung des Grundrechts auf Datenschutz eingetreten ist.

Die Gruppe berät die Kommission bei allen Vorhaben mit Datenschutzbezug mit dem Ziel, die Beachtung des Rechts auf informationelle Selbstbestimmung bereits bei der europäischen Gesetzgebung bestmöglichst zu gewährleisten. Leider haben die jeweiligen Arbeitseinheiten der Kommission bisweilen den Datenschutzbezug nicht oder erst verspätet erkannt. Dies hatte zur Folge, dass eine angemessene Beteiligung der Artikel 29-Gruppe nicht stattfinden konnte und teilweise Regelungen beschlossen wurden, die erhebliche Datenschutzdefizite aufwiesen.



Da es eine besondere, unabhängige Datenschutzberatung im Ministerrat nicht gibt, ist eine Verbesserung der Kontakte zwischen dem Rat und der Artikel 29-Gruppe dringend erforderlich, um schlüssige Datenschutzstrategien und -normen zu fördern. Dies wäre um so wünschenswerter, als der Rat zunehmend Maßnahmen und Regelungen initiiert bzw. beschlossen hat, die den Datenschutz der europäischen Bürgerinnen und Bürger erheblich tangieren.

Parallel hierzu hat die Artikel 29-Gruppe ihre Zusammenarbeit mit den gemeinsamen Datenschutzkontrollgremien vertieft, die mit dem Schengener Übereinkommen, dem Europol- und dem ZIS-Übereinkommen und dem Eurojust-Beschluss des Rates errichtet wurden. Diese Zusammenarbeit stellt in gewisser Hinsicht einen Vorlauf der Initiativen für einen verbesserten Datenschutz der europäischen Polizei- und Justizbehörden dar, auf die weiter unten näher eingegangen wird.

Neue Technologien

Der technologische Datenschutz war stets ein zentrales Thema für die Artikel 29-Gruppe, wie schon ihre ersten Arbeitspapiere belegen (z.B. WP 6 Anonymität im Internet, WP 11 »Platform for Privacy Preferences (P3P)« und »Open Profiling Standard (OPS)«). Die Gruppe hat sich stets darum bemüht, beratend auf die datenschutzverträgliche Konzipierung und Umsetzung solcher Technologien hinzuwirken.

Die Gruppe konzentriert sich dabei auf zentrale Themen, insbesondere das Internet und seine Dienste (insb. WP 37), Funkchips (RFID – WP 105), neue Instrumente zur Durchsetzung von Rechten an geistigem Eigentum (WP 104) und zur mobilen und geografischen Ortung (WP 115) sowie die Entwicklungen auf dem Gebiet der elektronischen Behördendienste (WP 73 eGovernment).

Die Gruppe verfolgt aber auch wissenschaftliche und technologische Entwicklungen in anderen Bereichen, wie z. B. der Genetik (WP 91) oder der Biometrie (insbesondere die Aufnahme biometrischer Daten in Ausweise und Reisedokumente aber auch ihre Integration in länderübergreifende Informationssysteme wie Eurodac, Europol, Schengener Informationssystem, Visa-Informationssystem – WP 110).

Internationale Übermittlung personenbezogener Daten

Nach Inkrafttreten der Richtlinie im Jahr 1998 entwickelte sich die internationale Datenübermittlung zu einer der wichtigsten Datenschutzfragen. Bedeutsam ist dabei insbesondere die Frage der Angemessenheit des Datenschutzes in Drittländern (hierzu bereits WP 4 und viele weitere). Hier gibt es einen viel versprechenden Ansatz: verbindliche Unternehmensregelungen (Binding Corporate Rules – BCR), mit denen multinationale Unternehmen ausreichende Datenschutzgarantien bei der weltweiten konzerninternen Datenübermittlung anbieten können (vgl. WP 107, 108).

Die Artikel 29-Gruppe verfolgt auch die Arbeiten im Europarat und der Arbeitskreise der OECD zum Datenschutz, der Datensicherheit und zum Schutz der Persönlichkeitsrechte.

Zunehmend an Bedeutung gewinnt die Förderung des Datenschutzes in Lateinamerika, Asien und Afrika. Die Gruppe versucht, diese Länder bzw. Regionen darin zu bestärken, ihren Bürgerinnen und Bürgern Datenschutzgarantien zu geben mit der »Nebenwirkung«, dass der Datenaustausch zwischen den EU-Staaten und diesen Drittländern erheblich vereinfacht wird.

Schließlich hat die Gruppe Initiativen ergriffen, um den transatlantischen Dialog und die Kontakte mit Datenschutzkontrollgremien in Kanada und den Vereinigten Staaten zu fördern. Erst kürzlich ist mit der Federal Trade Commission, die in den USA die Einhaltung des Safe Harbor Abkommens überwacht, ein regelmäßiger Meinungsaustausch verabredet worden.

Herausforderungen durch den internationalen Terrorismus und seine Bekämpfung

Für die Gruppe waren die letzten Jahre von dem andauernden dramatischen Konflikt um das Verhältnis von Sicherheit und Freiheitsrechten geprägt. Auf der einen Seite standen die zahlreichen Versuche von Regierungen, neue Mittel im Kampf gegen den Terrorismus einzuführen. Auf der anderen müssen die datenschutzrechtlichen Grundsätze als wesentlicher Bestandteil der Freiheit und der Demokratie verteidigt werden. Die vorgeschlagenen und teilweise bereits umgesetzten Maßnahmen betreffen sowohl die »Erste Säule« (Binnenmarkt) als auch die »Dritte Säule« (justizielle und polizeiliche Zusammenarbeit). Die Artikel 29-Gruppe ist offiziell ein Teil der Ersten Säule. In der Dritten Säule gibt es – bislang – kein gleichwertiges Gremium zur Beratung. Dies Defizit verstärkt das Risiko, dass die Auswirkungen für den Datenschutz nicht angemessen berücksichtigt werden.

Die vom Rat und von der Kommission unternommenen Initiativen im Bereich der polizeilichen und justiziellen Zusammenarbeit betrafen verschiedene Maßnahmenpakete. Hinzuweisen ist insbesondere auf

- den Transfer von Passagierdaten in die USA (WP 87, 95, 97, 103). Die Gruppe äußerte sich zufrieden darüber, dass das EP die kritische Sicht zu den entsprechenden Vereinbarungen der Kommission mit den USA teilt.
- Vorschläge zum Visa-Informationssystem (WP 110).
- Die Einführung biometriegestützter Pässe (WP 112).
- Verschiedene Initiativen zum intensiveren Datenaustausch zwischen Polizei- und Justizbehörden (WP 116).
- Die europaweite generelle und anlasslose Verpflichtung zur Speicherung von Telekommunikationsdaten (WP 109, 113).

Ich sehe es positiv, dass der kürzlich vorgelegte Kommissionsvorschlag für einen Rahmenbeschluss zum Datenschutz in der »Dritten Säule« Vorgaben für einen harmonisierten Datenschutz für die Justiz und Polizei enthält. Hierzu gehört auch die Einsetzung eines Gremiums der unabhängigen Datenschutzbehörden für die »Dritte Säule«, dessen Status und Aufgaben im wesentlichen denjenigen der Artikel 29-Gruppe für die »Erste Säule« entsprechen. Es ist zu hoffen, dass dieses neue Rechtsinstrument bald beschlossen wird, um einen angemessenen Datenschutz bei der polizeilichen Zusammenarbeit zu erreichen.

Schlussfolgerungen

Die Artikel 29-Gruppe ist zwar nicht das einzige Datenschutzgremium auf EU-Ebene, sicherlich aber das wichtigste. Deutlich ist, dass sich das Spektrum ihrer Arbeit in den letzten Jahren ständig erweitert hat. Dies gilt vor allem im Hinblick auf die Initiativen zur intensiveren Zusammenarbeit in der »Dritten Säule« der EU, also von Polizei und Justiz. Aber auch bezüglich der rasanten technologischen Entwicklung ergeben sich immer neue datenschutzrechtliche Fragen.

Dem Selbstverständnis der Artikel 29-Gruppe entspricht es dabei, sinnvolle Entwicklungen und erforderliche Entscheidungen nicht zu blockieren, sondern so zu gestalten, dass neben einer rein fachlichen Sicht auch die fundamentalen Datenschutzanforderungen berücksichtigt werden. Letztlich geht es darum, das Grundrecht auf Datenschutz europa- und weltweit zu etablieren und mit Leben zu erfüllen. Dabei sieht sich die Artikel 29-Gruppe als Sachwalterin der Bürgerinnen und Bürger, deren personenbezogene Daten in einer Welt des ständigen technologischen und datenschutzrechtlichen Wandels in immer größerem Umfang verarbeitet werden.

Die Gruppe ist sich darüber im klaren, dass sie diese ambitionierten Ziele nicht im Alleingang erreichen kann, sondern nur zusammen mit anderen politischen und gesellschaftlichen Akteuren. Hierzu zählen neben den erwähnten Institutionen auch Verbände und Medien. Dabei können und müssen die Datenschützer verstärkt die Kooperation mit Interessenvertretern suchen, die in bestimmten Bereichen (ggf. aufgrund der jeweiligen Interessenlage) an einem guten Datenschutz interessiert sind. Beispiele hierfür sind die Zusammenarbeit mit der Telekommunikationswirtschaft bei der Auseinandersetzung um die Vorratsspeicherung, die Kooperation mit Gewerkschaften beim Arbeitnehmerdatenschutz und mit Verbraucherschützern beim Datenschutz in elektronischen Diensten.

Umfrage

Gleichbehandlung beim Gesinnungstest

Nach einer Umfrage von TNS Infratest für den Spiegel zu dem in Baden-Württemberg eingeführten Gesinnungstest für muslimische Einbürgerungswillige (s.u. S. 30) antworteten auf die Frage: »In Baden-Württemberg werden seit Jahresanfang einbürgerungswilligen Muslimen Fragen zu politischen und gesellschaftlichen Themen gestellt. Wer sollte diese Fragen Ihrer Meinung nach beantworten müssen?«

- alle Einbürgerungswillige 70 %
- niemand 16 %
- nur Muslime 9 %

(Der Spiegel 3/2006, 20)

Karin Schuler

Europäische Datenschutzorganisationen

Bürgerrechtsorientierte Datenschutzorganisationen außerhalb Deutschlands in Europa - eine Übersicht

Datenschutz und Bürgerrechte ganz allgemein können nicht mehr nur innerhalb nationaler Grenzen geschützt und erhalten werden. Wenn Konzerne ebenso wie Regierungen grenzenlose Datensammlungen aufbauen, verwenden und austauschen, müssen Bürgerrechtler und Datenschützer auf Augenhöhe kämpfen. Dazu ist eine stärkere europäische und internationale Vernetzung notwendig.

Obwohl es bereits vielfältige Ansätze zu grenzüberschreitender Zusammenarbeit (z. B. bei den Big Brother Awards) gibt, fehlt eine wirklich schlagkräftige europäische Datenschutzorganisation, die auch auf europäischer Gesetzgebungsebene wirksam Lobbyarbeit für den Datenschutz betreiben könnte.

Die folgende Liste zeigt nicht nur, dass die Ansätze der Organisationen so vielfältig wie die Versuche zu internationaler Zusammenarbeit sind. Sie zeigt leider auch, dass es in einigen europäischen Ländern außer den offiziellen Datenschutzbehörden keine organisierte nationale Datenschutzlobby auf Bürgerrechtsebene zu geben scheint.

Belgien

Association Electronique Libre (AEL)

www.ael.be

Belgische Vereinigung, die sich dem Grundrechtsschutz in der Informationsgesellschaft widmet. Sie unterstützt Sprach-, Presse- und Versammlungsfreiheit im Internet, das Recht auf Verschlüsselung, das Recht auf monopolfreie Softwareentwicklung und das Recht auf freien Informationszugang.

Die AEL unterhält eine große Zahl vom Mailinglisten in englischer und französischer Sprache, ein WIKI (digitales Lexikon) zum Thema »Grundrechte in der Informationsgesellschaft« und unterstützt open source- und free software-Projekte.

European Digital Rights (EDRI)

www.edri.org

Europäische Organisation belgischen Rechts, die sich seit 2002 dem Erhalt bürgerlicher Rechte in der Informationsgesellschaft widmet. EDRI versteht sich als Dachorganisation für seine Mitglieder, die ihrerseits Bürgerrechtsorganisationen aus europäischen Staaten sind.

EDRI engagiert sich in Fragen, die auf europäischer Ebene diskutiert und reguliert werden, wie z.B. Vorratsdatenspeicherung, Abhörbefugnisse, Copyright, Beschränkung von Internet-Zugängen und -Inhalten, cyber crime und Überwachungsanforderungen.

Zweiwöchentlich informiert der elektronische Newsletter EDRI-gram über die Situation digitaler Rechte in Europa.

Vorstand: Ian Brown, Rikke Frank Joergensen, Andreas Krisch, Lena Nalbach, Sjoera Nas.

Finnland

Electronic Frontier Finland (EFFI ry)

www.effi.org

Finnische Organisation, die seit 2001 finnische Bürgerinnen und Bürger bei der Wahrnehmung ihrer Rechte im Cyberspace unterstützt. Sie widmet sich dabei insbesondere Themen wie informationelle Selbstbestimmung, Redefreiheit und Urheberrechten.

EFFI ist Gründungsmitglied der EDRI und unterhält diverse Mailinglisten in finnischer Sprache. Sie verleiht außerdem die jährlichen finnischen Big Brother Awards.

Dänemark

Digital Rights

www.digitalrights.de

Dänische Bürgerrechtsorganisation, die sich seit 2000 der Sensibilisierung in Hinblick auf den Erhalt von Bürgerrechten im Internet widmet.

Digital Rights ist eng verbunden mit der europäischen Organisation EDRI, deren Gründungsmitglied sie ist.

Frankreich

Imaginons un Réseau Internet Solidaire (IRIS)

www.iris.sgdg.org

Eine französische Organisation, die sich seit 1997 dem Erhalt bürgerlicher Rechte bei der Nutzung elektronischer Ressourcen widmet. Dabei befasst sie sich hauptsächlich mit den politischen und gesellschaftlichen Aspekten der Internet-Nutzung. Sie unterstützt ganz besonders den freien Zugang zum Internet zur nicht-kommerziellen Nutzung.

IRIS ist Gründungsmitglied von EDRI.

Geschäftsstelle: Samuel Chabert, Jaques Dufresne, Georges Malamoud, Kais Marzouki, Meryem Marzouki, Francois Sauterey

Großbritannien

Liberty

www.liberty-human-rights.org.uk

Eine britische Organisation, die sich dem Schutz und Erhalt von Bürgerrechten widmet. Datenschutz ist dabei eines ihrer Betätigungsfelder.

Liberty wurde 1934 als National Council for Civil Liberties gegründet

und setzt sich seitdem für Menschen- und Bürgerrechte ein.

Liberty nimmt Einfluss durch Lobbying und Sachverständigentätigkeit bei der Gesetzgebung, Durchführung von Musterprozessen, Forschungsprojekten und Gutachten, Weiterbildungsangebote und Kampagnen (z. B. gegen die Einführung eines Personalausweises in Großbritannien).

Die Organisation wird durch einen 35-köpfigen Rat (council) geführt bei gleichzeitig hoher Einflussnahmemöglichkeit durch die Mitglieder. Sie unterhält eine sehr serviceorientierte Website und ist insgesamt recht professionell organisiert.

Privacy International
www.privacyinternational.org

Eine unabhängige Bürgerrechtsorganisation, die im Jahre 1990 gegründet wurde und als Wächter vor Überwachung und Überwachungstendenzen in Staat und Gesellschaft warnt. Der Hauptsitz von PI ist in London, aber es gibt eine starke Bindung in die USA: PI selbst hat in Washington ein eigenes Büro und ist außerdem eng mit der amerikanischen Bürgerrechtsorganisation Electronic Privacy Information Center (EPIC) verbunden, mit der sie auch eine gemeinsame Website (www.privacy.org) betreibt. PI legt Wert auf eine möglichst internationale Ausrichtung und hat aus diesem Grund einen Beirat internationaler Experten.

PI engagiert sich in allen Bereichen, die mit der Überwachung von Menschen als Bürger, Verbraucher oder Arbeitnehmer einhergehen durch Kampagnen, Forschung und Veranstaltungen. PI gibt gemeinsam mit EPIC den jährlichen Bericht »Privacy & Human Rights Survey« heraus.

Statewatch
www.statewatch.org

Statewatch wurde 1991 in London als nicht-kommerzielle, ehrenamtliche Organisation gegründet. Ihre Mitgliedschaft ist vielfältig: es sind Rechtsanwälte, Akademiker, Journalisten, Wissenschaftler und Bürgerrechtler vertreten. Statewatch versteht sich als europäisches Netzwerk, das in 14 Ländern präsent ist und sich hauptsächlich um die kritische Berichterstattung über Staat, Justiz, Innenpolitik, und Bürgerrechte bemüht. In Deutschland besteht eine Kooperation mit der Redaktion Bürgerrechte & Polizei/CILIP.

Statewatch versteht sich in erster Linie als Informationsbeschaffer, um Bürgerinnen und Bürgern solide Entscheidungsgrundlagen für eigene politische Einschätzungen zu liefern.

Diverse regelmäßige Veröffentlichungen und Mailinglisten sollen hierzu beitragen, u. a. das Statewatch bulletin, die Statewatch news, die SEMDOC website und andere.

Island

Mannvernd
www.manvernd.is/english

Mannvernd ist eine ehrenamtliche Organisation, die sich gegen den Aufbau einer vollständigen isländischen medizinischen (und auch genetischen) Datenbank durch eine private Organisation zur Wehr setzt.

Sie wurde von Wissenschaftlern, Medizinern und anderen besorgten Bürgerinnen und Bürgern gegründet, um die durch die gesetzlich beschlossene Totalerfassung bedrohten Bürgerrechte zu stärken.

Italien

ALCEI
www.alcei.org

Electronic Frontiers Italy wurde 1994 in Mailand gegründet. Der Name steht für Associazione per la Libertà nella Comunicazione Elettronica Interattiva. ALCEI hat enge Kontakte zur amerikanischen Electronic Frontier Foundation, ist aber eine eigenständige Organisation.

ALCEI versteht sich als international tätige Bürgerrechtsvereinigung und ist Gründungsmitglied der Global Internet Liberty Campaign (GILC – www.gilc.org).

Niederlande

Bits of Freedom
www.bof.nl

Bits of Freedom ist eine niederländische, ehrenamtliche Organisation mit Sitz in Amsterdam. Sie widmet sich hauptsächlich den Themen Datenschutz und digital rights. Schwerpunkte sind Copyright, das Spannungsfeld zwischen Strafverfolgung und Datenschutz, Redefreiheit und SPAM. Bits of Freedom gibt einen regelmäßigen Newsletter heraus und verleiht jährlich die niederländischen Big Brother Awards. BOF ist außerdem Gründungsmitglied von EDRI.

Österreich

Arge Daten
www.argedaten.at (leider nur mit Javascript vernünftig nutzbar)

Österreichische Gesellschaft für Datenschutz, die sich seit 1983 mit Fragen des Informationsrechts, des Datenschutzes, der Telekommunikation und des Einsatzes neuer Techniken befasst. Der Verein ist parteipolitisch unabhängig und als gemeinnützig anerkannt.

Die Arge Daten widmet sich dem menschengerechten und gesellschaftlich verantwortbaren Einsatz von Informationstechnik und Telekommunikation und unterstützt die Einhaltung und Weiterentwicklung des Rechts auf informationelle Selbstbestimmung.

Sie gibt einen regelmäßigen Informationsdienst (Mailingliste »Privacy Weekly«) heraus und beteiligt sich neben ihren eigenen Aktivitäten auch an Kooperationsprojekten, wie z. B. den A-Cert Zertifizierungsdienst für Digitale Signaturen.

Ukraine

Privacy Ukraine
www.internetrights.org.ua

Privacy Ukraine wurde 1999 als nicht-kommerzielle Organisation in Kiew gegründet, die sich dem Datenschutz, der Meinungsfreiheit und Informationsfreiheit widmet. Die Organisation hat anfänglich insbesondere daran mitgewirkt, die nationale Gesetzgebung an die europäischen Standards anzupassen.

Dr. Thilo Weichert

Wo liegt Prüm? Der polizeiliche Datenaustausch in der EU bekommt eine neue Dimension

Am 27. Mai 2005 wurde in Prüm ein internationaler Vertrag zwischen den EU-Mitgliedstaaten Deutschland, Spanien, Frankreich, Luxemburg, Holland, Österreich und Belgien unterzeichnet. In dieser ratifizierungsbedürftigen Vereinbarung sehen die Partner einen verstärkten und erleichterten polizeilichen Datenaustausch vor. Dieser Vertrag soll und kann dazu beitragen, dass die grenzüberschreitende Strafverfolgung und die Gefahrenabwehr verbessert werden. Dabei werden Datenschutzfragen aufgeworfen, die – wenn sie nicht beantwortet werden können – zum Bumerang nicht nur für die Bürgerrechte, sondern auch für die Polizei werden können. Im Folgenden wird der Vertrag dargestellt und aus Datenschutzsicht bewertet.

I. Einführung

Prüm liegt in Rheinland-Pfalz, nicht sehr weit entfernt von dem noch kleineren luxemburgischen Grenzort Schengen, der inzwischen europaweit über das Schengen-Vertragswerk und das Schengener Informationssystem (SIS) bekannt geworden ist. Der Vertrag von Prüm ist kein Bestandteil des Schengenvertrags und soll auch kein Teil des in die EU-Strukturen integrierten Schengen-Acquis werden. Doch folgt er dem Modell der Schengen-Zusammenarbeit, bevor diese im Amsterdam-Vertrag von 1999 in die erste und die dritte Säule der EU integriert wurde: Eine Gruppe von EU-Kernstaaten einigen sich außerhalb der formellen Strukturen der EU auf eine engere Zusammenarbeit mit dem erklärten Ziel, die auf einer multilateralen Ebene entwickelten Regeln in die EU hineinzutragen. Daraus folgt auch, dass das Europäische Parlament während der zwischenstaatlichen Phase nichts zu sagen hat. Es wird auch nur noch einen begrenzten Einfluss haben, wenn die sieben Staaten – oder inzwischen einige mehr – ihre Regeln in die EU integrieren wollen. Nach Art. 51 des Vertrags von Prüm können – nach Akzeptieren der vorgegebenen Regeln – sämtliche EU-Mitgliedstaaten dem Vertrag von Prüm beitreten.

Die Einbeziehung in die EU-Strukturen soll spätestens drei Jahre nach Inkrafttreten des Vertrages erfolgen, also nach Ratifizierung des Prümer Vertrages durch die sieben nationalen Parlamente. Während dieser Zeit werden die Vertragsparteien die Umsetzungsvereinbarungen ausarbeiten, in denen die technischen Details festgelegt werden, z.B. die Einrichtung der Kontaktstellen, die technische Verknüpfung der Datenbanken oder die Form der Übermittlung der zusätzlich vermittelten Daten.

II. Verfügbarkeit versus Datenschutz

Der Vertrag muss im Zusammenhang gesehen werden mit den Bestrebungen innerhalb der EU, das so genannte »Prinzip der Verfügbarkeit« (principle of availability) zu verwirklichen. Dieses sieht einen weitgehenden und möglichst unbeschränkten Datenaustausch zwischen den Strafverfolgungs- und Polizeibehörden in den EU-Mitgliedsstaaten vor. Dabei handelt es sich um Pläne, die nach den Bombenanschlägen von Madrid am 11.03.2004 entwickelt worden sind (Vorschlag für einen Rahmenbeschluss des Rates über den Austausch von Informationen nach dem Grundsatz der Verfügbarkeit, KOM -2005- 490 eng. Ratsdok. 1341/05 = BR-Drs. 770/05). Konkret verpflichten sich die Mitgliedstaaten, gleichwertigen Strafverfolgungsbehörden und Europol die Daten zur Verfügung zu stellen, »die diese zur Erfüllung ihrer gesetzlichen Aufgaben im Hinblick auf die Verhütung, Aufdeckung und Untersuchung von Straftaten benötigen«. Zu diesem Zweck werden gegenseitige Online-Zugriffe auf Strafverfolgungsdateien eröffnet. Zugegriffen werden soll zunächst auf folgende Daten: DNA-Profile, Fingerabdrücke, Kfz-Halterdaten, Telekommunikationsbestands- und Verbindungsdaten sowie Identifizierungs- und Personenstandsdaten. Soweit die online angebundenen Verfahren Indexdateien sind, sollen auch die Dokumente beschafft werden können, auf die hingewiesen wird. Rechtsstaatliche Sicherung sind in dem geplanten Rahmenbeschluss nicht vorgesehen.

Das Prinzip der Verfügbarkeit soll die traditionellen Formen des Datenaustauschs in ihrer Logik in ihr Gegenteil umkehren: Bisher wird in Verträgen geregelt, welche Daten unter welchen Bedingungen ausgetauscht werden dürfen. Dies gilt selbst noch für die weit reichenden und kritikbedürftigen Regelungen in der Europol-Konvention. Dem gegenüber geht das Prinzip der Verfügbarkeit davon aus, dass grundsätzlich alle Daten weitergegeben werden können.

Zwar folgte diesem Rahmenbeschluss einige Monate später im Oktober 2005 – eher als Beweis schlechten Gewissens denn als Indiz für die Grundrechtssensibilität – von der Kommission ein Vorschlag für einen »Rahmenbeschluss des Rates über den Schutz personenbezogener Daten, die im Rahmen der polizeilichen und justiziellen Zusammenarbeit in Strafsachen verarbeitet werden« (KOM -2005- 475 endg. 2005/0202 -CNS). Doch würde auch dieses Dokument den Datenschutz im Bereich Justiz und Inneres nicht wesentlich verbessern. Es ergeht sich wortreich in allgemeinen Grundsätzen des Datenschutzes, um schließlich jede Datenverarbeitung zu erlauben, die nach nationalem Recht zugelassen wird und die »zur Verhütung, Aufdeckung, Untersuchung und Verfolgung von Straftaten oder zur Abwehr einer Bedrohung der öffentlichen Sicherheit oder einer Person erforderlich« ist und keine »Interessen oder Grundrechte der betroffenen Person

überwiegen«. Durch diese Abwägungsklausel wird es letztendlich den beteiligten Polizeibehörden überlassen, die Betroffeneninteressen durch eigene Strafverfolgungsbelange auszustechen.

Der Entwurf des Rahmenbeschlusses zum Polizeidatenschutz nimmt keine Unterscheidung zwischen Strafverfolgung und Gefahrenabwehr vor. Jedes Bagatelldelikt kann den Austausch und die Nutzung von Daten legitimieren, selbst wenn dieses Delikt in einem der beteiligten Staaten nicht strafbar ist. Zwar wird zwischen verschiedenen Rollen der Betroffenen differenziert, also z.B. nach Eigenschaft als Täter, Verdächtiger, Opfer, Hinweisgeber, Sonstiger. Doch werden hieraus keine materiellrechtlichen Konsequenzen gezogen. Die Anwendbarkeit für Daten aus Akten wird ausgeschlossen. So lässt sich der Datenschutz in der Dritten Säule der EU nicht gewährleisten.

Der Grundgedanke der Verfügbarkeit liegt dem Vertrag von Prüm insofern zu Grunde, als er ein generelles Zugangs- und Abrufrecht zu Registern und Datenbanken der Vertragsstaaten gewährt und zusätzlich die Möglichkeit eröffnet, weitere Informationen und Erkenntnisse abzufordern.

III. Der Abgleich von DNA-Profilen

Alle Vertragsstaaten verpflichten sich zur Einrichtung von forensischen DNA-Datenbanken. Ebenso wie bei den Fingerabdrucksystemen (z.B. dem deutschen »Automatisierten Fingerabdruckidentifikationssystem« – AFIS) werden die digital verformelten DNA-Daten mit Namensangaben einer bestimmten Person oder bei Spuren mit Angaben zu einem bestimmten Sachverhalt/einer bestimmten Straftat in einer Datenbank gespeichert. Spurendaten sind als solche registriert. Art. 2 beschreibt die inhaltlichen Anforderungen an die nationalen DNA-Datenbanken, ohne aber Datenschutzbestimmungen festzulegen. Zugriffsfähig sind damit grundsätzlich extensive Datenbanken wie die britische, bei denen Speicherungen auch im Bagatellbereich und auf Verdachtsbasis erfolgen, sowie solche, bei denen höhere materiellrechtliche und verfahrensrechtliche Voraussetzungen vorliegen müssen. Als einzige Schranke ist normiert, dass die Daten nur für Zwecke der Strafverfolgung ausgetauscht werden dürfen und nicht für präventive Polizeizwecke. Die digitalen DNA-Profile (Fundstellendatensätze) dürfen nicht auf codierenden Genabschnitten beruhen.

Die entsprechenden DNA-Datenbanken werden den anderen Vertragsstaaten zugänglich gemacht. Die Fundstellendatensätze werden vollständig zum Abgleich zur Verfügung gestellt. Im Fall eines »Treffers« erhält die anfragende nationale Kontaktstelle automatisiert eine Meldung mit Hinweis auf die Kennung. Die weitere Kommunikation bzw. der weitere Datenaustausch erfolgt über die nationalen Kontaktstellen, denen eine ähnliche Rolle zukommt wie den SIRENE-Büros beim Schengen-System. Die weitere Übermittlung von den zu den Fundstellendatensätzen vorhandenen personenbezogenen Daten erfolgt nach dem innerstaatlichen Recht, insbes. den Vorschriften über die Rechtshilfe der ersuchten Vertragspartei (Art. 5), soweit diese Daten verfügbar sind. Art. 7 regelt ergänzend, dass Vertragsstaaten Rechtshilfe bei der Gewinnung molekulargenetischen Materials und der Übermittlung von DNA-Profilen leisten, wenn sich die gesuchte Person auf dem jeweiligen Territorium befindet. Voraussetzung ist, dass die DNA-Analyse sowohl nach dem Recht des ersuchten wie nach dem des ersuchenden Landes zulässig ist.

IV. Fingerabdrücke (daktyloskopische Daten)

Der Vertrag erlaubt in Art. 8 den gegenseitigen Zugriff auf daktyloskopische Daten und Hinweisdaten (Kennung), die jedoch keine identifizierenden Daten enthalten dürfen. Auf das Recht des abgebenden Staates kommt es nicht an, so dass sich die anfragende Polizei nicht mit dessen Recht auseinandersetzen muss. Die präzise Zuordnung des Fingerabdrucks erfolgt nach Übermittlung der Fundstellendatensätze durch die abrufende Stelle. Als Zweck sind nicht nur die Strafverfolgung, sondern auch die Gefahrenabwehr (Verhinderung von Straftaten) zugelassen. Der Datenaustausch im Trefferfall ist vergleichbar geregelt wie bei DNA-Treffern (Art. 10).

V. Kfz-Fahrzeug- und -Halterdaten

Den nationalen Kontaktstellen der anderen Vertragsstaaten wird zum Zweck der Strafverfolgung und umfassend der Gefahrenabwehr sowie zur Verfolgung von Ordnungswidrigkeiten, für die die Staatsanwaltschaft oder Gerichte zuständig sind, der automatisierte Einzelabruf von Eigentümer- bzw. Halterdaten sowie von Fahrzeugdaten aus nationalen Registern erlaubt (Art. 12). Voraussetzung ist die Verwendung des vollständigen Kennzeichens bzw. der vollständigen Kfz-Identifizierungsnummer. Die Abfrage muss mit dem Recht des abrufenden Vertragsstaates vereinbar sein.

VI. Politische Demonstrationen und Großveranstaltungen (Art. 13-15)

Die Zusammenarbeit in diesem Bereich geht bis in die 80er Jahre zurück. Sie wurde in den 90er Jahren zunächst innerhalb der Schengen-Gruppe geregelt, dann im Rahmen des Rates der EU zum Gegenstand einer Gemeinsamen Aktion gemacht. Dabei erfolgte die Einrichtung von nationalen Kontaktstellen; Verbindungsoffiziere wurden in den Staat mit dem Großereignis gesandt; Informationen wurden ausgetauscht. Der während des G-8-Gipfels in Genua im Jahr 2001 praktizierte personenbezogene Informationsaustausch – einschließlich der Übermittlung von »schwarzen Listen« – wird nun legalisiert. Daten können spontan oder auf Anfrage ausgetauscht werden für Zwecke der Gefahrenabwehr oder Strafverfolgung. Wie die Praxis von Genua zeigte, kann dies z.B. Vorbeugegewahrsam, Inhaftnahme oder Einreiseverweigerung zur Folge haben.

VII. Übermittlung zur Verhinderung terroristischer Straftaten (Art. 16)

Diese Form des Austauschs besteht seit den späten 70er Jahren und geht auf die TREVI-Zusammenarbeit zurück. Kontaktstellen waren die Staatsschutzpolizeien. Die Kommunikation erfolgte zunächst über ein geschlossenes Fax-Netz, das später unter dem Begriff »BDL-Netzwerk« bekannt wurde. BDL bedeutet »bureau de liaison« (Verbindungsbüro). Es ist nicht eindeutig erkennbar, was sich in diesem Bereich mit dem Prüm-Vertrag ändern soll.

Namen, weitere Identifikationsdaten sowie sonstige Angaben dürfen übermittelt werden, soweit dies erforderlich ist, weil bestimmte Tatsachen die An-

nahme rechtfertigen, dass die Betroffenen Straftaten nach den Art. 1-3 des Rahmenbeschlusses 2002/475/JI des EU-Rates vom 13.06.2002 zur Terrorismusbekämpfung begehen werden. Der automatisierte Abgleich darf im Einzelfall nach Maßgabe des innerstaatlichen Rechts des abrufenden Staates erfolgen. Die Übermittlung setzt keine Anfrage voraus. Entsprechendes ist nach Art. 46 des Schengener Durchführungsabkommens schon zulässig, ohne dass dort die Beschränkung auf den Rahmenbeschluss des EU-Rates bestünde. Erfasst sind nicht nur terroristische Anschläge, sondern auch extremistische Bestrebungen oder etwa auch politisch begründete Aktionen zivilen Ungehorsams.

Die übermittelnde Stelle kann die Übermittlung mit Nutzungsbeschränkungen für die empfangende Stelle versehen. Diese Beschränkungen können sich auf eine Nutzung als Gerichtsbeweis oder im Rahmen einer konkreten strafrechtlichen Ermittlung beziehen. Sie sind üblich, wenn die Informationen von Informanten, von verdeckten Ermittlern, aus Abhöraktionen oder aus dem Einsatz besonderer Ermittlungstechniken stammen. Vor allem Staatsschutzabteilungen und Geheimdienste haben oft ein gesteigertes Interesse am Schutz bzw. am Verbergen ihrer Quellen.

VIII. Sonstige Regelungsbereiche

Art. 17 und 18 haben keine Datenschutzrelevanz. Sie erlauben den Einsatz von bewaffneten Flugsicherheitsbegleitern (sky marshals) in Luftfahrzeugen. Kapitel 4 (Art. 20-23) des Vertrages bezieht sich auf die Bekämpfung illegaler Migration, u.a. den Einsatz von Verbindungsbeamten und Dokumentenberatern. Der Austausch über »Erkenntnisse zur illegalen Migration« kann sich nur auf allgemeine Informationen beziehen; ein personenbezogener Austausch wird mit der Regelung des Art. 20 Abs. 2 nicht erlaubt. Die in Art. 23 normierte Unterstützung bei Rückführungen erfolgte schon in der Vergangenheit (z.B. bei der vom deutschen Bundesgrenzschutz praktizierten Rückführung von 17 afrikanischen Asylsuchenden gemeinsam mit belgischen und schweizer Behörden). Auch insofern legitimieren die neuen Regelungen nicht zu einem erweiterten Austausch von Personendaten.

Art. 24 regelt die Intensivierung der polizeilichen Zusammenarbeit durch gemeinsame Einsatzformen, wobei – nach Maßgabe des innerstaatlichen Rechts – fremde Polizeibeamte mit der Wahrnehmung hoheitlicher Befugnisse betraut werden können. Weitere Regelungen betreffen die Nacheile (Art. 25) und die Hilfeleistung bei Großereignissen, Katastrophen und Unglücksfällen (Art. 26). Eine weiter gehende grenzüberschreitende Polizeizusammenarbeit hat Deutschland z.B. mit der Schweiz durch Vertrag vom April 1999 verabredet (von gemeinsamen Streifen bis hin zu Verhaftungsrechten).

In Art. 27 verpflichten sich die Vertragsstaaten auf Ersuchen zur gegenseitigen Hilfeleistung auch in personenbezogenen Fällen unter Bezugnahme auf die Schengener Vertragsregelungen.

IX. Datenschutz

Kapitel 7 des Vertrags von Prüm (Art. 33 bis 41) enthält Bestimmungen zum Datenschutz. Dabei werden die allgemeinen international bestehenden Datenschutzdefinitionen und Prinzipien bekräftigt. Hinsichtlich des nationalen Datenschutzniveaus wird auf die Datenschutzkonvention des Europarates von 1981 und auf dessen Empfehlung zur Datenverarbeitung im Polizeibereich von 1987 Bezug genommen und zwar auch, soweit Daten nicht automatisiert verarbeitet werden (Art. 34). In Anlage 2 zum Vertrag von Prüm kommen die Vertragsstaaten in einer gemeinsamen Erklärung überein, »dass die Voraussetzungen für die Übermittlung von personenbezogenen Daten nach Kapitel 7 des Vertrages, soweit diese nicht den automatisierten Abruf oder Abgleich betreffen, im Wesentlichen bereits zum Zeitpunkt der Unterzeichnung vorliegen«, bzw. »dass sie hinsichtlich der noch fehlenden Voraussetzungen nach Kapitel 7 insbesondere im Bereich des automatisierten Abrufs oder Abgleichs, diese schnellst möglich schaffen werden«.

Art. 35 regelt – über die o.g. allgemeinen Regelungen hinausgehend – die Zweckbindung der nach dem Vertrag übermittelten Daten. Dabei wird festgelegt, dass die zum automatisierten Abruf genutzten Daten ausschließlich für den jeweiligen konkreten Einzelfall (und für Datenschutzzwecke) genutzt werden dürfen und danach – außer im materiell begründeten »Trefferfall« – unverzüglich gelöscht werden müssen.

Jede Übermittlung nach dem Vertrag muss für Zwecke der Datenschutzkontrolle protokolliert werden. Diese für zwei Jahre zu speichernden Daten dürfen ausschließlich für Zwecke der Datenschutzkontrolle und zur Gewährleistung der Datensicherheit genutzt werden (Art. 39).

Gemäß Art. 41 informiert die empfangende Vertragspartei »die übermittelnde Vertragspartei über die Verarbeitung der übermittelten Daten und des dadurch erzielten Ergebnisses«. Es ist dabei nicht ausdrücklich klargestellt, dass diese Informationen ausschließlich für Datenschutzzwecke genutzt werden dürfen.

X. Bemerkungen zum Vertrag

Der Vertrag von Prüm enthält aus Datenschutzsicht Licht und Schatten. Zu begrüßen ist grundsätzlich das Datenschutzregime mit einer umfassenden Protokollierungspflicht und einer bzgl. der Protokolldaten geltenden strengen Zweckbindung. Zugleich erfolgt mit dem Vertrag aber ein Paradigmenwechsel bei der polizeilichen Zusammenarbeit, indem die Datenbanken der Polizei zum gegenseitigen Abruf bereit gestellt werden. Bezüglich des Datenschutzniveaus bei den Abfragern wird letztendlich auf das dort geltende nationale Datenschutzrecht verwiesen. Als Mindeststandard werden die Empfehlungen des Europarates aus dem Jahr 1987 (!) herangezogen, die ausdrücklich nicht den Anspruch auf Verbindlichkeit erheben. Mehr als dies: Ohne ersichtliche tatsächliche Prüfung wird unterstellt, dass das Datenschutzniveau in den beteiligten Ländern schon ausreichend sein dürfte. Und sollte dies nicht der Fall sein, so versprechen sich die Partner – ohne Verbindlichkeit und Kontrolle – nachzubessern. Defizite sollen jedenfalls kein Hindernis für den Datenaustausch schon am Tag nach dem Inkrafttreten des Vertrags sein. Selbst wenn der derzeit als Entwurf vorliegende EU-Rahmenbeschluss für den Datenschutz im Bereich der Strafverfolgung anwendbar würde (s.o. II.), könnte kaum eine materielle Verbesserung erreicht werden.

Datenschutz und polizeilicher Datenaustausch sind zwei Dinge, die in der Praxis wenig miteinander zu tun haben müssen. Wer die polizeiliche Datenverarbeitung in Deutschland kennt und die Nichtbeachtung der Kenn-

zeichnungs- und Zweckbindungspflichten, der wird begründete Zweifel haben, dass sich dies in Deutschland nach Inkrafttreten des Vertrages von Prüm ändern wird und dass dem in den anderen Vertragsstaaten Folge geleistet werden wird.

Der Vertrag von Prüm ist insofern ein weiterer Beleg eines äußerst beklagenswerten Umstandes – des Fehlens von verbindlichen Datenschutzstandards innerhalb der EU im Bereich der dritten Säule. Während bzgl. des Datenaustauschs und sonstiger Ermittlungen der Polizei immer mehr Befugnisse eingeräumt werden – jeweils angestoßen durch spektakuläre internationale Straftaten – entwickeln die EU und die nationalen Regierungen keine ernsthaften Anstrengungen zur Gewährleistung gemeinsamer verbindlicher Datenschutzregelungen und eines einheitlichen Verfahrens. Schlimmer noch beim Vertrag von Prüm: Durch Abschluss eines völkerrechtlichen Vertrages – außerhalb der EU-Strukturen – werden sämtliche EU-Institutionen ausgeschlossen. Dies hat fatale Konsequenzen für die rechtliche wie die parlamentarische Kontrolle: die europäischen Gerichte und das Europäische Parlament sind nicht zuständig. Die nationalen Organe und Gremien können ihre theoretisch zustehenden Kontroll- und Einspruchsmöglichkeiten de facto nicht wahrnehmen.

Der Vertrag von Prüm ist im Internet verfügbar unter www.statewatch.org/news/2005/jul/schengenIII-german-full.pdf. Die Anlagen dazu befinden sich unter www.statewatch,org/news/2005/jul/schengenIII-german-Anl2.pdf.

Dokumentation

179. Sitzung der Innenministerkonferenz – Karlsruher Erklärung

Am 8. und 9. Dezember 2005 fand in Karlsruhe auf Einladung des baden-württembergischen Innenministers Heribert Rech als Vorsitzenden unter dem Motto »Mit Sicherheit was los« die 179. Sitzung der Innenministerkonferenz (IMK) statt.

Die Terroranschläge von Madrid und London hätten gezeigt, dass sich auch Deutschland auf mögliche Anschläge vorbereiten müsse. Obgleich es bis heute keine Anzeichen einer konkreten Gefährdung gäbe, zeige die Entführung von Susanne Osthoff im Irak, dass Deutsche nicht vom internationalen Terrorismus verschont blieben. »Wir dürfen uns nicht in Sicherheit wiegen« betonte Heribert Rech in einer Presseerklärung.

Daher begrüße die Innenministerkonferenz, dass nach dem Koalitionsvertrag schnellstmöglich eine Anti-Terror-Datei geschaffen werden solle.

Neben einem Dialog zwischen muslimischen Organisationen und Sicherheitsbehörden empfehle die IMK, nachdem in Madrid als auch in London der öffentliche Personennahverkehr Ziel der Anschläge gewesen sei, vermehrt Haltestellen und Fahrzeuge mit Videokameras zu überwachen. Wichtig sei aber auch die Früherkennung von geplanten Anschlägen. Durch eine Aufklärungskampagne würden die Betreiber von Verkehrsbetrieben sowie die Fahrgäste für die Gefahr sensibilisiert. »AUFMERKSAM UNTERWEGS! Mit dieser Kampagne wollen wir erreichen, dass auf herrenlose Gepäckstücke geachtet wird und verdächtige Beobachtungen dem Aufsichts- und Sicherheitspersonal sofort mitgeteilt werden«, sagte Rech. Mit Plakaten, Anzeigen, Videospots auf elektronischen Werbeflächen der Verkehrsbetriebe bis hin zu Lautsprecherdurchsagen wolle man die Wachsamkeit der Fahrgäste erhöhen.

Die enge Zweckbindung der von Autobahn-Mautstellen erfassten Daten müsse zur Verbrechensbekämpfung gelockert werden. Da es ausschließlich um Straftaten von erheblicher Bedeutung gehe, seien die Belange des Datenschutzes gewahrt, sagte Rech.

Weitere Themen auf der Konferenz waren die Hilfe beim Wiederaufbau der afghanischen Polizei, die Ausländerpolitik, die Fußball-Weltmeisterschaft, die Bekämpfung des Rechtsextremismus, Drogen im Straßenverkehr, der Missbrauch von EC-Karten sowie Soft-Air- und Anscheinswaffen.

Die Innenminister und -senatoren der Länder und des Bundes haben das Positionspapier »Karlsruher Erklärung« des IMK-Vorsitzenden zu Fragen der Freiheit, der Sicherheit und des Rechts zur Kenntnis genommen:

Karlsruher Erklärung

»Die Innenminister und -senatoren der Länder und des Bundes bekennen sich zu einem auf dem Subsidiaritätsprinzip basierenden bürgernahen Europa, das den Anliegen und Bedürfnissen der Bürgerinnen und Bürger Rechnung trägt. Die Innenminister und -senatoren begrüßen die Europäische Union als einen einzigartigen Raum der Freiheit, der Sicherheit und des Rechts in dem Bewusstsein, dass insbesondere vor dem Hintergrund einer weltweiten terroristischen Bedrohungslage kein Mitgliedstaat für sich allein mehr in der Lage ist, die Sicherheit seiner Bürgerinnen und Bürger in vollem Umfang zu gewährleisten. [...]

Die Innenminister und -senatoren nehmen zu den nachfolgenden Themenbereichen aus ihrem Zuständigkeitsbereich Stellung:

I. Innere Sicherheit

Die Europäische Union steht auch im Hinblick auf die Innere Sicherheit vor großen Herausforderungen. Der internationale Terrorismus, grenzüberschreitende und internationale organisierte Kriminalität, illegale Migration und Schleuserbanden, gewalttätige reisende Hooligans und Kriminalität im Internet sind herausragende Beispiele der aktuellen Bedrohungs- und Sicherheitslage, auf die die Mitgliedstaaten der Europäischen Union mit Nachdruck und fester Entschlossenheit reagieren müssen. [...]

Europa stellt auch in kriminalgeografischer Hinsicht einen einheitlichen Raum dar, der staatenübergreifend eng

vernetzte Kriminalitätsstrukturen aufweist. Die Innenminister und -senatoren vertreten die Auffassung, dass Europa die sich daraus ergebenden sicherheitspolitischen Herausforderungen nur meistern kann, wenn sich jeder einzelne Mitgliedstaat mit seinem Handeln und Unterlassen seiner Verantwortung für die Sicherheit der Bürgerinnen und Bürger in der gesamten Europäischen Union bewusst ist.

Dieser bereits in den Schengener Verträgen verankerte zentrale Gedanke muss stets Leitlinie und tragendes Fundament der europäischen Innenpolitik sein. Deshalb ist es nach Auffassung der Innenminister und -senatoren notwendig, alle Kräfte zu bündeln und die Europäische Union gemeinsam zu einer großen Sicherheitsunion auszubauen, in der sich alle Partner zu ihrer Verpflichtung für das große Ganze bekennen. Gerade deshalb ist es auch unverzichtbar, die Personenkontrollen an den Binnengrenzen mit den neuen und künftigen Mitgliedstaaten erst aufzuheben, wenn diese die Sicherheitsstandards der Union dauerhaft gewährleisten können und deren erfolgreiche Umsetzung in der Praxis vor Ort überprüft worden ist. [...]

Dabei muss es vorrangiges Ziel sein, neue polizeiliche Kooperationsformen zu vereinbaren, die eine umfassende, schnelle, unkomplizierte und reibungslose grenzüberschreitende Zusammenarbeit ermöglichen und insoweit den Bedürfnissen und Anforderungen der polizeilichen Praxis in vollem Umfang Rechnung tragen. Die Innenminister und -senatoren betonen, dass bestehende Hemmnisse im Interesse einer effektiven Bekämpfung der internationalen Kriminalität weiter abgebaut werden müssen. Dabei ist eine Orientierung an den Inhalten der wegweisenden neuen Staatsverträge mit der Schweiz, mit Österreich und den Niederlanden sowie des Vertrages von Prüm über die »Vertiefung der grenzüberschreitenden Zusammenarbeit, insbesondere zur Bekämpfung des Terrorismus, der grenzüberschreitenden Kriminalität und der illegalen Migration« zielführend.

Ungeachtet des negativen Ausgangs der letzten Referenden zum Europäischen Verfassungsvertrag ist nach Auffassung der Innenminister und -senatoren eine zügige Umsetzung des Haager Programms zur Ausgestaltung der Zusammenarbeit im Bereich der Innenpolitik der nächsten Jahre anzustreben, soweit dies die herrschenden vertraglichen und politischen Bedingungen zulassen.

Hierzu zählen in erster Linie die eingehende Novellierung des Schengener Durchführungsübereinkommens. Damit einhergehend treten die Innenminister und -senatoren dafür ein, die operative polizeiliche Zusammenarbeit weiterzuentwickeln und die polizeilichen Rechtshilfebefugnisse deutlich auszuweiten. Im Hinblick auf die Verbesserung des polizeilichen Informationsaustauschs zwischen den Sicherheitsbehörden der Mitgliedstaaten durch die Umsetzung des im Haager Programm festgelegten Grundsatzes der Verfügbarkeit von Daten sind ferner die unionsweiten polizeilichen Datenbanken (insbesondere Schengener Informationssystem und Europol-Informationssystem) zu optimieren. Den Sicherheitsbehörden ist der Zugriff auf das Visa-Informationssystem VIS einzuräumen. Außerdem ist eine Vernetzung der polizeilichen Datensysteme der Mitgliedstaaten, wie beispielsweise der DNA- und Fingerabdruck-Datenbanken, dringend anzustreben und baldmöglichst zu realisieren. Schließlich müssen weitere Anstrengungen zur Bekämpfung des internationalen Terrorismus unternommen werden. So sind beispielsweise die Anbieter von Kommunikationsdiensten zur Protokollierung und temporären Speicherung bestimmter Verbindungsdaten zu verpflichten.

Die operationelle Kompetenz von Europol ist nach Auffassung der Innenminister und -senatoren weiter auszubauen, damit Europol künftig seiner Schlüsselrolle als Service- und Unterstützungsstelle der mitgliedstaatlichen Polizeien bei der unionsweiten Bekämpfung der grenzüberschreitenden Kriminalität gerecht werden kann.

Vor dem Hintergrund der mitunter globalen Dimension der Bedrohungspotenziale ist auch eine Verbesserung und Intensivierung der internationalen Kooperation im Polizei- und Justizbereich anzustreben, insbesondere im Hinblick auf die Zusammenarbeit von Europol und Interpol.

Die Innenminister und -senatoren begrüßen mit Blick auf die Qualität der Außengrenzen der Europäischen Union, dass die Europäische Grenzagentur mit Sitz in Warschau am 1. Mai 2005 mit der Wahrnehmung wichtiger Querschnittsaufgaben (Risikoanalyse, Harmonisierung der Aus- und Fortbildung, Förderung der Entwicklung von Detektionstechnik, Koordinierung gemeinsamer Rückführungsmaßnahmen) begonnen hat. [...]

III. Migrations- und Flüchtlingspolitik

[...] Die Innenminister und -senatoren unterstützen die Forderung nach einer gemeinsamen Visapolitik mit der Zielsetzung, die Dokumentensicherheit zu verbessern und die angelaufenen Arbeiten zur Aufnahme von biometrischen Daten in Reise- und Identitätsdokumente sowie in Visa und Aufenthaltstitel fortzuführen. Sie sind weiter der Auffassung, dass das Visa-Informationssystem (VIS) und das neue Schengener Informationssystem (SIS II) einen wesentlichen Beitrag nicht nur zur Verbesserung des Schutzes der Außengrenzen und der Rückführungsmöglichkeiten bei illegal aufhältigen Drittstaatsangehörigen, sondern auch zur Inneren Sicherheit, namentlich zur Bekämpfung des internationalen Terrorismus und der organisierten Kriminalität leisten können. Visa-Informationssystem und Schengener Informationssystem SIS II sollten so bald wie möglich in Betrieb genommen und umfassend genutzt werden. Das Ziel der nachhaltigen Verbesserung der Sicherheit innerhalb der Europäischen Union kann durch diese Systeme allerdings nur dann zufriedenstellend erreicht werden, wenn auch den Sicherheits- und den Ausländerbehörden eine umfassende Nutzung der erfassten Daten ermöglicht wird. [...]

Der von der Kommission vorgelegte Vorschlag für eine Richtlinie über gemeinsame Normen und Verfahren in den Mitgliedstaaten zur Rückführung illegal aufhältiger Drittstaatsangehöriger wird den Erfordernissen einer Bekämpfung illegaler Migration aber nicht gerecht. Er formuliert lediglich die Ausgestaltung von Schutzrechten und überbetont damit einseitig die Interessen illegal aufhältiger Drittstaatsangehöriger. [...]

Die Innenminister und -senatoren begrüßen, dass die Europäische Union nach Vorlage einer entsprechenden Studie der Kommission die Möglichkeit einer den ganzen Schengenraum einbeziehenden Registrierung aller Einreisen von Drittstaatsangehörigen in und Ausreisen aus dem Schengenraum prüfen wird. Eine solche Registrierung brächte mit Blick auf die damit verbundene Möglichkeit zur Überwachung von Aufenthaltszeiträumen einen erheblichen sicherheitspolitischen Gewinn. [...]«

Dr. Patrick Breyer:

Vorratsdatenspeicherung – Die totale Protokollierung der Telekommunikation kommt

Jede Benutzung von Telefon, Handy und Internet wird künftig protokolliert, damit die Strafverfolgungsbehörden auf diese Informationen zugreifen können. Dies sieht ein Beschluss des Europäischen Parlaments vom Dezember 2005 vor. Doch welche Auswirkungen hat eine solche Vorratsdatenspeicherung?

1. Einführung

Die Bedeutung des Begriffs »Vorratsspeicherung von Telekommunikationsdaten« erschließt sich nicht von selbst, ist aber schnell erklärt: Telekommunikationsdaten geben Aufschluss darüber, wer wann mit wem und von welchem Ort aus kommuniziert hat, sei es per Telefon, Handy oder Internet. Die Verwendungsmöglichkeiten dieser Daten sind enorm: Mithilfe von Telekommunikationsdaten können grobe Bewegungsprofile erstellt, geschäftliche Kontakte rekonstruiert und Freundschaftsbeziehungen identifiziert werden. Das Wissen über den jeweiligen Kommunikationspartner kann zudem Rückschlüsse auf den Inhalt der Kommunikation, auf persönliche Interessen und Einstellungen zulassen. So braucht es nicht viel Fantasie, um die Bedeutung einer Email an eine AIDS-Beratungsstelle oder eines Telefonats mit einem auf Steuerstrafrecht spezialisierten Rechtsanwalt zu erkennen. Wegen der weitgehenden Verwendungs- und Missbrauchsmöglichkeiten von Kommunikationsdaten ist ihre Aufzeichnung und Aufbewahrung bisher nur insoweit zulässig, wie es zu Abrechnungszwecken unbedingt erforderlich ist.

2. Vorratsspeicherungs-Richtlinie

Am 14. Dezember 2005 hat das Europaparlament nun dem Entwurf einer Richtlinie zur Vorratsspeicherung von Kommunikationsdaten zugestimmt. In Zukunft müssen Telekommunikationsunternehmen Informationen über Telefon-, Mobiltelefon-, Internet- und Emailverbindungen sowie über die Identität der Beteiligten mindestens sechs Monate lang aufbewahren. Damit soll erreicht werden, dass der Staat zur »Ermittlung, Feststellung und Verfolgung von schweren Straftaten« auf diese Daten zugreifen kann. Von der ursprünglichen Zielsetzung der Richtlinie, den Umgang mit Telekommunikationsdaten in Europa zu vereinheitlichen, ist nichts übrig geblieben. Die Richtlinie schreibt lediglich Mindeststandards vor. Den EU-Mitgliedsstaaten bleibt es unbenommen, die Daten länger speichern zu lassen, anderen Behörden zu weiteren Zwecken Zugriffsrechte einzuräumen oder weitere Datentypen speichern zu lassen.

Der Katalog der zwingend zu speichernden Datentypen ist lang. Immerhin müssen Kommunikationsinhalte nicht gespeichert werden. Ausgenommen sind damit etwa SMS-Nachrichten, Email-Betreffzeilen und die Adressen (URLs) aufgerufener Internetseiten. Noch wichtiger ist, dass nur ohnehin erfasste Daten auf Vorrat gespeichert werden müssen. Insbesondere Informationen über die Identität der Kunden müssen also nicht erhoben werden; es besteht keine Identifizierungspflicht. Deutschland hat 2004 allerdings »freiwillig« eine Identifizierungspflicht für Festnetz- und Mobilfunkanschlüsse eingeführt.

3. Diskussion

3.1. Argumente der Befürworter

In der Diskussion um die Vorratsdatenspeicherung argumentieren die Befürworter, die Maßnahme sei zur Bekämpfung von Kriminalität und Terrorismus erforderlich. Bei der Aufklärung der Anschläge auf Madrid im Jahr 2004 etwa hätten Telekommunikationsdaten einen entscheidenden Beitrag geleistet. Zum Schutz des Lebens potenzieller Opfer von Terroranschlägen und anderer Straftaten müssten alle verfügbaren Mittel ausgeschöpft werden. Die Vorratsspeicherung von Telekommunikationsdaten stelle keinen unverhältnismäßigen Eingriff in die Bürgerrechte dar. Die Inhalte der Telekommunikation würden nicht erfasst. Verbindungsdaten würden bereits heute zu Abrechnungszwecken gespeichert. Der staatliche Zugriff auf die Daten unterliege hohen Voraussetzungen und sei nur im Einzelfall nach gerichtlicher Anordnung zulässig. Unschuldige Bürger hätten deswegen nichts zu befürchten.

Diese Argumente sollen im folgenden einer kritischen Würdigung unterzogen werden.

3.2. Effektivität

Vor allem die Erforderlichkeit einer Vorratsdatenspeicherung ist in Frage zu stellen. Bereits heute haben Ermittler Zugriff auf Verbindungsdaten, die zu Abrechnungszwecken gespeichert sind. Im Bedarfsfall kann zusätzlich die Aufzeichnung der Kommunikationsdaten Verdächtiger angeordnet werden. Die erfolgreiche Aufklärung der terroristischen Anschläge in Madrid weist darauf hin, dass die gegenwärtige Verfügbarkeit von Kommunikationsdaten ausreicht und eine systematische, vorsorgliche Speicherung jedermanns Daten ganz regelmäßig nicht erforderlich ist.

Auf Vorrat gespeicherte Kommunikationsdaten können den Strafverfolgern in einzelnen Fällen zwar nützlich sein, allerdings in der Regel nur bei unvorsichtigen Kleinkriminellen. Heinz Kiefer, Präsident des Europäischen Verbands der Polizei, warnt: »Für Kriminelle bliebe es einfach, mit relativ sim-

plen technischen Mitteln eine Entdeckung zu verhindern, z.B. durch den Einsatz und häufigen Wechsel im Ausland gekaufter, vorausbezahlter Mobiltelefonkarten. Das Ergebnis wäre ein enormer Aufwand mit wenig mehr Wirkung auf Kriminelle und Terroristen, als sie etwas zu verärgern.«

Eine Vorratsdatenspeicherung wirkt sogar kontaproduktiv, weil sie die Entwicklung und den Einsatz von Anonymisierungstechniken fördert und der Polizei auf diese Weise selbst in Fällen schwerster Gefahr die Möglichkeit erfolgversprechender Ermittlungen abschneidet. Klaus Jansen, Vorsitzender des Bundes Deutscher Kriminalbeamter, klagt bereits heute: »Da es sich herumgesprochen hat, dass Telefongespräche relativ leicht abgehört werden können, reden die Verdächtigen nur noch selten offen am Telefon«. Wenn die Vorratsspeicherung kommt, werden sich Kriminelle auch darauf schnell einrichten.

Dass die Massenspeicherung von Kommunikationsdaten den Ermittlungsbehörden in einzelnen Fällen nützlich sein könnte, bedeutet zudem nicht, dass sie unseren Schutz vor Straftaten verbessern würde. Vor der Untersuchung dieser Frage ist es zunächst einmal wichtig, sich das reale Ausmaß unserer vielbeschworenen »Bedrohung« durch Kriminalität vor Augen zu halten: Eurostat zufolge sterben weniger als 0,002% der Europäer jährlich als Opfer einer Straftat, terroristische Anschläge eingeschlossen. Der Statistik zufolge ist es um ein Vielfaches wahrscheinlicher, im Straßenverkehr, durch einen Sturz oder wegen eines ungesunden Lebensstils (z.B. falsche Ernährung, Bewegungsmangel, Alkohol, Nikotin) zu sterben als infolge einer Straftat. Auch dass uns Zivilisationsrisiken wie Krankheit, Armut, Arbeitslosigkeit oder Naturkatastrophen treffen, ist weitaus wahrscheinlicher als das Risiko, Opfer einer Straftat zu werden.

Die Strafverfolgungsbehörden aller Industriestaaten der Welt gewährleisten bereits heute einen guten Schutz vor Straftaten, ohne dass Informationen über die Kommunikation der gesamten Bevölkerung aufgezeichnet werden müssten. Die Telekommunikationsüberwachung im Bedarfsfall hat in der Vergangenheit stets genügt. Selbst die USA kennen keine Vorratsspeicherungspflicht. Erst in den letzten Jahren haben einzelne europäische Staaten wie Irland generelle Speicherungspflichten eingeführt, ohne dass dies aber einen Einfluss auf die Kriminalitätsrate dieser Staaten gehabt hätte. Somit ist nicht erkennbar, dass eine Vorratsspeicherung einen besseren Schutz vor Straftaten gewährleistet.

Die hypothetische Eignung einer Vorratsdatenspeicherung zur Bekämpfung selbst schwerwiegendster Gefahren kann die Maßnahme nicht rechtfertigen. Straftaten und Gefahren drohen fast immer und überall. Angesichts der Fülle von Untaten in aller Welt ließe sich jederzeit auf die Gefahr eines terroristischen Anschlags verweisen, um auf diese Weise einen permanenten Ausnahmezustand zu definieren, der die Grundrechte dauerhaft einschränkt oder außer Kraft setzt.

Wenn die Befürworter der Vorratsspeicherung argumentieren, dass möglichst jeder Einzelfall aufgeklärt und jedes Opfer geschützt werden müsse, dann verkennen sie die Möglichkeiten und überhaupt das Wesen des Rechtsstaates. Vollständige Sicherheit ist in der Realität leider nicht herstellbar. Selbst autoritäre Regimes mit einem umfassenden Spitzelsystem wie die DDR waren nie in der Lage, umfassend vor Straftaten zu schützen. Ein solcher Anspruch würde ohnehin der historisch schmerzhaft gewonnenen Erkenntnis widersprechen, dass der Versuch eines möglichst lückenlosen Schutzes vor Straftaten letztendlich nicht im Interesse unserer Gesellschaft liegt. Ein Staat, der unbegrenzte Aktivitäten zum Schutze seiner Bürger entfalten würde, wäre kein freiheitlicher mehr. Eine Politik der Null-Toleranz hieße, private Freiheiten der Sicherheit zu opfern.

Es ist eine Errungenschaft unseres Rechtsstaates, dass zum Schutz der Unschuldigen, aber auch der Menschenwürde, auf bestimmte Mittel verzichtet wird, selbst wenn dies Nachteile für die Effektivität der Aufgabenerfüllung durch die Eingriffsbehörden mit sich bringt und sogar irreversible Schäden an Rechtsgütern – sei es auch durch terroristische Anschläge – nicht verhindert werden können. Die individuellen und unveräußerlichen Rechte jedes Menschen setzen dem Schutzanspruch des Staates Grenzen, wie etwa das vieldiskutierte Folterverbot verdeutlicht.

Langfristig dienen rechtsstaatliche Beschränkungen und die Achtung der Menschenrechte der Sicherheit, denn exzessive Kontrolle und Repression erzeugten Unzufriedenheit und Widerstand. Der Oberste Gerichtshof des Staates Israel führte im Jahr 1999 zutreffend aus: »Dies ist das Schicksal der Demokratie, weil nicht alle Mittel mit ihr vereinbar und nicht alle Methoden ihrer Feinde für sie verfügbar sind. Obwohl eine Demokratie oft mit einer Hand auf ihren Rücken gebunden kämpfen muss, behält sie trotzdem die Oberhand. Die Erhaltung der Rechtsstaatlichkeit und die Anerkennung der Freiheit des Einzelnen bilden einen wichtigen Bestandteil ihres Verständnisses von Sicherheit. Letztlich erhöht dies ihre Stärke.«

3.3. Wirtschaftliche Auswirkungen

In Zeiten des Haushaltsnotstands, einer schwachen Binnennachfrage und Bemühungen um »Bürokratieabbau« sollten auch die wirtschaftlichen Auswirkungen einer Vorratsdatenspeicherung nicht außer Acht bleiben. Die Kosten der Maßnahme werden für jedes größere Telekommunikationsunternehmen auf einmalig 180 Mio. Euro und auf jährlich weitere 50 Mio. Euro Betriebskosten geschätzt. Diese Zusatzkosten könnten die Telefon-, Handy- und Internetnutzung für den Verbraucher um 15 bis 20% verteuern.

In Deutschland scheint die Politik die finanziellen Auswirkungen der Vorratsdatenspeicherung indessen kaum zu beachten, weil die gesamten Kosten den betroffenen Unternehmen aufgebürdet werden sollen. Die Verfassungsgerichte Österreichs und Frankreichs haben jedoch bereits entschieden, dass die einseitige Abwälzung solcher Strafverfolgungskosten auf die Wirtschaft verfassungswidrig ist. Das Bundesverfassungsgericht prüft derzeit die entsprechende Regelung des deutschen Telekommunikationsgesetzes.

Müsste der Staat für die enormen Kosten der Vorratsdatenspeicherung aufkommen, würde er auf die Maßnahme wohl verzichten. Denn in diesem Fall würde offenbar, dass der damit verbundene Aufwand zulasten anderer, gezielter Maßnahmen zur Gewährleistung der Sicherheit ginge und dass die Mittel sinnvoller und effektiver zum Schutz der Bevölkerung eingesetzt werden könnten. Zur Eindämmung der Netzkriminalität beispielsweise versprechen technische Schutzmaßnahmen und Aufklärungskampagnen einen weitaus größeren Erfolg als repressive Maßnahmen.

3.4. Risiko falscher Verdächtigung

Untersucht man die Verhältnismäßigkeit einer generellen Aufzeichnung von Kommunikationsdaten, dürfen auch die negativen Auswirkungen dieser Maßnahme auf die Sicherheit der Bürger nicht außer Acht bleiben. Als »Verdachtsschöpfungsinstrument« erhöht eine Vorratsspeicherung das Risiko, zu Unrecht einer Straftat verdächtigt zu werden. Zur Aufklärung einer Brandstiftung in Schleswig-Holstein beispielsweise wurden anhand von Telekommunikationsdaten alle Besitzer eines Mobiltelefons ermittelt, die sich zur Tatzeit in der Nähe des Brandorts aufhielten. Die Polizei kündigte die Vernehmung all dieser Personen an. Auch sind Fälle bekannt, in denen Mobiltelefone gestohlen oder Internetzugänge »gehackt« worden waren und dadurch die berechtigten Besitzer bzw. Nutzer in den falschen Verdacht einer Straftat gerieten.

Ein falscher Verdacht kann einschneidende Folgen für den Betroffenen haben. Er kann zur Befragung von Nachbarn und Arbeitskollegen führen, zu einer Observation, zu Wohnungsdurchsuchungen oder zur Festnahme. Auch unberechtigte Aus- und Einreiseverweigerungen, Vermögensbeschlagnahmen, Grenzzurückweisungen wegen Namensverwechselungen bis hin zu Verschleppungen durch Geheimdienste und irrtümlichen Tötungen durch Polizei oder »Sky-Mashalls« sind Realität. Eine generelle Speicherung von Telekommunikationsdaten erhöht die Gefahr falscher Verdächtigungen, weil die Daten inhaltlich nur beschränkt aussagekräftig sind und der Benutzer des jeweiligen Geräts nicht sicher feststellbar ist. Die Vorratsdatenspeicherung wird dadurch selbst zum Sicherheitsrisiko.

3.5. Abschreckung erwünschten Verhaltens

Hinzu kommt das Risiko eines Missbrauchs der Daten durch Polizeibeamte, staatliche Behörden, Mitarbeiter von Telekommunikationsunternehmen oder Dritte. Eine Reihe von Vorfällen in der Vergangenheit hat gezeigt, dass ein Missbrauch sensibler Daten immer wieder vorkommt. Um uns effektiv vor Datenmissbrauch zu schützen, muss die Vorratsspeicherung von Kommunikationsdaten von vornherein untersagt werden. Andernfalls werden sich manche, die auf die Hilfe eines Arztes, eines Rechtsanwalts, eines Psychologen oder einer Beratungsstelle angewiesen sind, dadurch abschrecken lassen, dass ihr Kontakt noch monatelang nachvollzogen und sensible Informationen über ihr Privatleben in falsche Hände geraten können. Auch Informanten von Journalisten, die anonym staatliche Missstände aufdecken möchten, werden es in Zukunft schwer haben. Doch nicht nur das Redaktions-, Anwalts- und Arztgeheimnis wird beeinträchtigt. Die Nachvollziehbarkeit von Geschäftskontakten wird auch der Wirtschaftsspionage Vorschub leisten.

Das Bundesverfassungsgericht hat wiederholt davor gewarnt, dass eine exzessive Kommunikationsüberwachung die Unbefangenheit der Kommunikation beeinträchtigt und dadurch letztlich unserer Gesellschaft insgesamt schadet: »Die Befürchtung einer Überwachung mit der Gefahr einer Aufzeichnung, späteren Auswertung, etwaigen Übermittlung und weiteren Verwendung durch andere Behörden kann schon im Vorfeld zu einer Befangenheit in der Kommunikation, zu Kommunikationsstörungen und zu Verhaltensanpassungen [...] führen.«

Irreführend ist die Behauptung, Verbindungsdaten würden bereits heute zu Abrechnungszwecken gespeichert. Tatsächlich dürfen bisher nur abrechnungsrelevante Verbindungsdaten gespeichert werden. Nicht zulässig ist unter anderem die Aufzeichnung von Daten über die Internet- oder Emailnutzung oder über die Position von Mobiltelefonen. Außerdem können Kunden bislang die sofortige Löschung der gewählten Zielrufnummern nach Rechnungsversand wählen. All dies ändert sich durch eine Vorratsspeicherungspflicht.

3.6. Dammbruch

Wenn von deutscher Seite betont wird, dass ein Zugriff auf die gespeicherten Kommunikationsdaten nur eingeschränkt zulässig sein wird, mag dies zwar für die Gegenwart zutreffen. Eine Vielzahl von Beispielen in der Vergangenheit zeigt aber, dass man die nützlichen Datenbestände schon bald zu weiteren wichtigen Zwecken freigeben wird. Je nach Anlass werden Innenpolitiker die Nutzung der Daten zum Beispiel für Maßnahmen gegen Hooligans, zur Bekämpfung des Terrorismus durch Nachrichtendienste, zur Ahndung von Steuerhinterziehung, Urheberrechtsverletzungen oder auch Verkehrsdelikten fordern.

Die verdachtslose Massendatenspeicherung stellt im Kern einen Präzedenzfall für eine verdachtsunabhängige, flächendeckende maschinelle Überwachung und Kontrolle der Bevölkerung dar. Die fortschreitende Entwicklung des Überwachungsstaats reicht von der maschinellen Registrierung der Bevölkerung (biometrische Pässe und Ausweise, Meldewesen) über die permanente Aufzeichnung ihres Verhaltens (Vorratsspeicherung, Überwachungskameras) bis hin zur automatisierten Jedermannüberwachung und -kontrolle (Kfz-Kennzeichenabgleich mit Fahndungsdaten, routinemäßige Rasterfahndung, Videoüberwachung mit Gesichtserkennung oder mit automatischer Erkennung auffälliger Bewegungen).

Mit den Argumenten der Befürworter der Vorratsdatenspeicherung ließen sich sogar George Orwells »Telescreens« (Videokameras) in jeder Wohnung rechtfertigen, solange auf die Aufnahmen nur im Fall schwerer Gefahren zugegriffen werden dürfte. Der Kampf gegen den Terror wird so zunehmend zum Kampf gegen den Bürger. Während der freiheitliche Rechtsstaat im Grundsatz der Gesetzestreue seiner Bürger vertraute, ist im »Sicherheitsstaat« prinzipiell jeder verdächtig, ein »Gefährder« zu sein. Unter der Prämisse eines solchen Generalverdachts ist es von der vorsorglichen Datenspeicherung nicht mehr weit zu vorsorglichen Platzverweisen, Ausreiseverboten oder Inhaftierungen (»Sicherungsgewahrsam«). Daran wird deutlich, dass die Vorratsdatenspeicherung einen Dammbruch der traditionellen Grenzen staatlicher Eingriffe in die Rechte unbescholtener Bürger darstellt.

3.7. Schlussfolgerung

Es wurde gezeigt, dass die Massenprotokollierung der Telekommunikation keinen verbesserten Schutz vor Kriminalität bieten wird. Stattdessen kostet sie hunderte Millionen Euro, gefährdet die Sicherheit Unschuldiger, beeinträchtigt vertrauliche Kommunikation und ebnet den Weg in eine immer umfangreichere Massenüberwachung und -kontrolle der Bevölkerung. Die Strafverfolgungsbehörden werden nur ei-

nen kleinen Bruchteil (etwa 0,0004%) der anfallenden Kommunikationsdaten jemals nachfragen. Sind demzufolge aber mehr als 99% der von einer Vorratsspeicherung Betroffenen unschuldig, dann kann die Maßnahme nicht mehr als verhältnismäßig angesehen werden.

4. Umsetzung und weitere Entwicklung

4.1. Gerichtliche Prüfung

Es ist zu hoffen, dass auch die Gerichte die Unverhältnismäßigkeit dieser Maßnahme erkennen und Gesetze zur Vorratsdatenspeicherung für verfassungswidrig erklären werden. Eine erste Gelegenheit dazu könnte ein Verfahren vor dem Europäischen Gerichtshof (EuGH) bieten, das Irland einzuleiten beabsichtigt. Irland hält die Richtlinie zur Vorratsdatenspeicherung für rechtswidrig, weil sie nicht in die Kompetenz der EG falle. Im Rahmen eines solchen Verfahrens könnte der Europäische Gerichtshof neben der Kompetenzfrage auch die Vereinbarkeit der Richtlinie mit den Gemeinschaftsgrundrechten prüfen, zu denen auch das Recht auf informationelle Selbstbestimmung zählt.

Gleichzeitig bereiten Bürgerrechts- und Verbraucherschutzorganisationen eine Verfassungsbeschwerde gegen das deutsche Gesetz zur Umsetzung der Vorratsspeicherungsrichtlinie vor. Voraussichtlich werden sich auch einige der zur Speicherung verpflichteten Unternehmen dem Verfahren anschließen. Wenn das Bundesverfassungsgericht die Vorratsdatenspeicherung für unverhältnismäßig hält, kann es zur Annullierung der Richtlinie den Europäischen Gerichtshof anrufen.

4.2. Forderungen

Für den Fall, dass sich der Bundestag trotz der vermutlichen Verfassungswidrigkeit der Maßnahme zur Einführung einer Vorratsdatenspeicherung in Deutschland entschließen sollte, muss dies so bürger- und wirtschaftsfreundlich erfolgen, wie es die Richtlinie zulässt. Insbesondere ist zu fordern:

1. Die maximale Umsetzungsfrist bis Mitte 2007 – für Internetdaten bis Anfang 2009 – ist auszuschöpfen.

2. Bürger dürfen nicht verpflichtet werden, sich vor der Nutzung von Telefon, Handy oder Internet zu identifizieren. Bestehende Identifizierungspflichten sind aufzuheben.

3. Eine Vorratsspeicherung wird nur für die in der Richtlinie genannten Datentypen und nur für die Dauer von sechs Monaten eingeführt; danach sind die Daten unverzüglich zu löschen. Zu speichern sind nur Daten, die bei dem jeweiligen Anbieter zur Bereitstellung von Kommunikationsdiensten ohnehin erzeugt oder verarbeitet werden.

4. Der Staat hat die zur Datenspeicherung und -vorhaltung verpflichteten Anbieter für die daraus resultierenden Zusatzkosten (Investitionskosten, Vorhaltekosten, Personalkosten) voll zu entschädigen.

5. Der staatliche Zugriff auf Informationen über die Kommunikation und die Kommunizierenden (»Verkehrsdaten«, »Bestandsdaten«) hat den gleichen Voraussetzungen zu unterliegen wie der Zugriff auf die Inhalte der Kommunikation.

6. Der Zugriff auf Kommunikationsdaten ist nur zur Verhinderung oder Verfolgung schwerer Straftaten zuzulassen, wenn im Einzelfall der konkrete Verdacht einer solchen Tat besteht. Der Zugriff zwecks Strafverfolgung sollte beschränkt sein auf Fälle organisierter Kriminalität, in denen eine höhere Strafe als vier Jahre Freiheitsstrafe zu erwarten ist.

7. Eine Nutzung von Kommunikationsdaten zu anderen Zwecken, beispielsweise durch Nachrichtendienste, durch sonstige Behörden oder durch private Dritte, ist auszuschließen. Die speichernden Diensteanbieter selbst sind zur Nutzung der Daten nur insoweit zuzulassen, wie es zur Entgeltermittlung und Entgeltabrechnung erforderlich ist.

8. Der Zugriff auf und die Verwertung von Informationen über die Kommunikation von Ärzten, Rechtsanwälten, Steuerberatern, anderen Berufsgeheimnisträgern sowie Journalisten sind nur in besonderen Ausnahmefällen zuzulassen.

9. Zur Datenspeicherung und -vorhaltung sind nur Anbieter öffentlich zugänglicher Kommunikationsdienste und Betreiber öffentlicher Kommunikationsnetze zu verpflichten. Kleine Anbieter, insbesondere im Internetbereich, sind auszunehmen.

10. Die positiven und negativen Auswirkungen der Vorratsdatenspeicherung auf die Gesellschaft sind von einer unabhängigen Stelle zu untersuchen. Die Ergebnisse sind zu veröffentlichen. Der Bundesdatenschutzbeauftragte hat dem Deutschen Bundestag alle zwei Jahre Bericht über die Erfahrungen mit der praktischen Anwendung der Vorratsdatenspeicherung zu erstatten. Die Berichte sind zu veröffentlichen.

Bei Anderen gelesen

Joschkas Form der infomationellen Selbstverteidigung

Der Spiegel berichtet über Joschka Fischers Rückzug aus der Politik und seine jüngsten Erfahrungen als Privatmann: »Vor vier Wochen hat er seine Freundin ... in Rom geheiratet. ... Für den Rückflug aus Rom hatte Fischer drei Tickets in einem Ferienflieger der Air Berlin gebucht. Er saß mit seiner Gattin und deren Tochter in der ersten Reihe, dort, wo sonst die Familien mit kleinen Kindern platziert werden. Plötzlich kam ein fremder Passagier nach vorn, baute sich mit seiner Kamera vor den Fischers auf und knipste das Paar für die »Bild«-Zeitung.
Fischer zitterte vor Wut. Kaum war der Paparazzo verschwunden, griff er den Fotoapparat seiner Frau und ging nach hinten. Er wollte den Mann mit seinen eigenen Waffen schlagen, er wollte seine Ehre zurückfotografieren. Der Mann hielt sich eine Zeitung vor das Gesicht, weil ihm die Enthüllung, die sein Geschäft ist, am eigenen Leibe peinlich war. Fischer zog die Zeitung beiseite und drückte ab. Die umsitzenden Passagiere klatschten. Wie nach einer geglückten Landung« (Beste/Feldenkirchen, Der Spiegel 48/2005, 35).

Dr. Thilo Weichert

Volkszählung 2010: Statistische Notwendigkeit oder gläserner Bürger?

Deutschland will sich, so die rot-schwarze Vereinbarung, am EU-weiten Zensus 2010/2011 beteiligen. Dies schlägt schon 5 Jahre zuvor Wellen. Eine Illusion sollten sich die Befürworter einer neuen Volkszählung nicht machen: Die Deutschen würden sich heute gerne durchleuchten lassen. Dies zeige sich schon daran, dass sie per Kredit- und Kundenkarten, Handy und Online-Einkauf ihre persönlichen Daten preisgäben. Die Deutschen sind sensibler was den Schutz ihrer informationellen Selbstbestimmung, was den Datenschutz betrifft als Angehörige anderer Nationalitäten. Eine Erklärung hierfür ist die schmerzhafte Erfahrung mit zwei Überwachungsstaaten. Liegt das Nazideutschland auch schon 60 Jahre zurück, die Stasi-Bespitzelung ist noch keine 20 Jahre her. Die deutsche Sensibilität erklärt sich auch mit den positiven Erfahrungen beim Widerstand gegen die Volkszählungen 1983 bzw. 1987, in denen erfolgreich gesellschaftliche Mitbestimmung bei der informationellen Selbstbestimmung eingefordert wurde.

Sicherlich hat sich seit den 80ern einiges geändert, nicht aber das Maß der Sensibilität. Es gibt ein Grundrecht auf Datenschutz. Dessen Schutz wurde – vorneweg durch das Volkszählungsurteil von 1983 – vom Bundesverfassungsgericht in vielen Urteilen konkretisiert. Elektronische Datenverarbeitung ist nicht mehr ein staatliches Privileg, sondern Alltag für die meisten Bundesbürgerinnen und -bürger. So ist das Misstrauen gegen den volkszählenden Staat auch nicht mehr so groß: Die erkämpften Standards des Datenschutzes – Abschottung der Statistik, Zweckbindung, verfahrensrechtliche Sicherung, Gesetzesvorbehalt, Transparenz – würden die Statistiker diesmal wohl schon aus Vernunftgründen einhalten.

Ob die Volkszählung nötig ist, um zu wissen, wieviel Menschen in Deutschland wo und wie leben, hierüber mag man unterschiedlicher Meinung sein. Es ist nun einmal die Aufgabe der Statistiker, möglichst genaue Zahlen zu haben. Deshalb aber eine Voll-Volkszählung durchzuführen, wie in den 80ern, wäre statistischer und ökonomischer Unsinn. Es gibt inzwischen wirksamere und kostengünstigere Methoden, an die nötigen Daten heranzukommen. Daher macht es viel Sinn, über den »registergestützten Zensus« nachzudenken. Dabei würden die vorhandenen Daten z.B. aus den Einwohnermeldeämtern, der Bundesagentur für Arbeit oder der Bundesversicherungsanstalt für Angestellte auf statistischer Ebene, d.h. pseudo- oder anonymisiert, zusammengespielt. Nur noch ergänzend würden Stichproben-Interviews mit den Menschen direkt durchgeführt. In Ländern mit qualifizierten Verwaltungs-Datenbanken funktioniert ein solcher Register-Zensus schon heute sehr gut, etwa in den Niederlanden oder in den skandinavischen Staaten.

Gegen den Register-Zensus wird eingewandt, unsere Verwaltungsregister seien zu fehlerhaft. Dies mag sein. Es gibt aber keinen Grund, diesen beklagenswerten Zustand beizubehalten. Tatsächlich macht es sehr viel Sinn, die Richtigkeit unserer Datenbanken zu verbessern. Doch darf dabei nicht der gleiche Fehler gemacht werden wie Anno 1983: die begründeten Sorgen und Ängste der Menschen müssen ernst genommen werden. Bei einer Registerbereinigung muss der Datenschutz der Bürgerinnen und Bürger beachtet werden. Dies bedeutet: Einbeziehung der Betroffenen, keine Koppelung der Datenkorrektur mit Sanktionen, Beachtung der Zweckbindung, keine zentralen zweckübergreifenden Datenbestände.

Das Problem besteht darin, dass in den bundesweiten Verwaltungsdateien bisher der Datenschutz zumeist ganz klein geschrieben worden ist. Für die Bundesagentur für Arbeit ist dieser Begriff bisher ein Fremdwort geblieben. Das alte Bundes-Wirtschaftsministerium wollte über das JobCard-Verfahren ein gewaltige Einkommensdatenbank der gesamten abhängig beschäftigten deutschen Bevölkerung schaffen, was definitiv verfassungswidrig wäre. Schon beschlossen ist eine einheitliche Steuer-Identifizierungsnummer, die die Menschen von der Geburt bis in den Tod begleitet und die als Personenkennzeichen genutzt werden kann. Auch dieses ist, so die derzeit einhellige Überzeugung, verfassungswidrig. Bei der Schaffung von E-Government-Standards, etwa der Einführung des biometrischen Passes und Ausweises, hat sich die Bundesregierung bisher nicht wirklich um den Datenschutz geschert. Hier muss sich etwas ändern.

Demonstriert die Bundesregierung, dass sie es bei ihren Verwaltungsdateien mit der informationellen Selbstbestimmung der Bürgerinnen und Bürger ernst meint, so wird sie auch eine Qualitätsverbesserung ihrer Register erreichen; ein Register-Zensus ist dann ebenso wenig ein Problem wie die Akzeptanz der Bevölkerung für eine Volkszählung. Allein: Der rot-schwarze Koalitionsvertrag ist kein Beleg dafür, dass die neue Bundesregierung diese Lektion schon kapiert hat. Sie muss erst noch ihre Hausaufgaben machen.

Woanders gelesen

Oettinger für Politiker-Privatsphäre

Als Günther Oettinger in den 80er Jahren - damals noch einfacher Landtagsabgeordneter - in eine Telefonabhöraktion bei dem von ihm oft frequentierten Italiener geriet und diese Abhörprotolle gegen ihn genutzt wurden, zeigte dieser CDU-Politiker schon hohe Sensibilität für Datenschuz und Fernmeldegeheimnis. Inzwischen ist er Ministerpräsident von Baden-Württemberg und gerade für 5 weitere Jahre gewählt, der seinen Anspruch auf Privatheit formuliert: »Wenn ein Regierender kein Privatleben hat, gehe ich raus« (Der Spiegel 7/2006, 40).

Kein betrieblicher Datenschutzbeauftragter für Kleinbetriebe?

Stellungnahme der DVD vom 01.12.2005 zum Gesetzentwurf des Bundestages zur Änderung des Bundesdatenschutzgesetzes vom 23.09.2005 (Drucksache 599/05)

Der Bundesrat hat einen Entwurf zur Änderung des Bundesdatenschutzgesetzes in den Bundestag eingebracht, in dem das Quorum zur Bestellung eines betrieblichen Datenschutzbeauftragten (bDSB) in kleinen Betrieben von 5 auf 20 Mitarbeiter erhöht werden soll.

In der Begründung gibt der Bundesrat folgende Ziele an:

1. Entlastung der verantwortlichen Stellen (»kleinere« personenbezogene Daten verarbeitende Unternehmen)
2. Entlastung der Aufsichtsbehörden
3. Beseitigung der Unklarheiten einer komplizierten Regelung
4. Entbürokratisierung
5. Senkung der Kosten in den Betrieben
6. Stärkung der Eigenverantwortung der Betriebe

Die DVD nimmt dazu wie folgt Stellung:

Die Begründung zum Änderungsvorschlag bezüglich des Schwellenwerts versäumt vollständig, die Rechte der von Datenspeicherung betroffenen Personen zu erwägen. Sämtliche Begründungen und Erwägungsgründe zielen ausschließlich auf die vermeintliche Erleichterung in der Betriebsführung der betroffenen Unternehmen und vermitteln den Eindruck, die Einhaltung von Datenschutz-Anforderungen sei wesentlich »lästige Pflicht«. Die Fokussierung auf die Sicht der betroffenen Unternehmen lässt Zweifel aufkommen, ob die grundgesetzlichen Verankerung des Schutzes der Persönlichkeitsrechte Betroffener überhaupt zur Kenntnis genommen wurde.

Der Sinn der Bestellung eines betrieblichen Datenschutzbeauftragten liegt in der Sicherstellung verfassungsmäßig garantierter Rechte und nicht in der Aufrechterhaltung einer bestimmten Anzahl meldepflichtiger oder zur Bestellung verpflichteter Unternehmen.

Die zutreffende Erkenntnis, dass wegen der heute umfangreicheren automatisierten Datenverarbeitung mehr Unternehmen zur Bestellung eines betrieblichen Datenschutzbeauftragten verpflichtet wären, beruht daher auf der schlichten Tatsache, dass mehr potenziellen Gefährdungen für die Betroffenen zu begegnen ist.

Die im Gesetzentwurf vorgestellte Lösung, wegen der gestiegenen Zahl der verpflichteten Unternehmen das Quorum zu erhöhen, um eine Anpassung an frühere, niedrige Zahlen zu erreichen, offenbart eine zumindest eigenwillige Auffassung, die die DVD aufs Schärfste kritisiert, da sie auf letztlich sachfremden Erwägungen beruht.

Den Betrieben wird mit der Gesetzesinitiative zudem ein völlig falsches Signal gesetzt: Es ist zu befürchten, dass sich als Essenz die Annahme »Datenschutz erst ab 20 Personen« festsetzt. Die Erreichung der in der Begründung genannten Ziele ist aus Sicht der DVD mit dem vorgestellten Gesetzentwurf nicht möglich.

Zu 1. – Entlastung der verantwortlichen Stellen

Der Bundesrat hebt in der Begründung hervor, dass die Entlastung einer großen Anzahl kleiner Unternehmen erzielt wird, weil sie keinen betrieblichen Datenschutzbeauftragten mehr bestellen müssen.

A. Die Gegenüberstellung der derzeitigen und der nach gegebenenfalls erfolgter Gesetzesänderung bestehenden Meldevoraussetzungen ist jedoch lückenhaft und unterstellt dadurch verzerrend eine wesentlich zu hohe Zahl zukünftig nicht mehr meldepflichtiger bzw. zur Bestellung eines bDSB verpflichteter Unternehmen:

- Unabhängig von der Größe des Unternehmens und der Anzahl der mit der Verarbeitung personenbezogener Daten beschäftigten Personen sind Unternehmen zur Meldung verpflichtet, wenn sie weder eine Einwilligung des Betroffenen noch ein Vertragsverhältnis oder vertragsähnliches Vertrauensverhältnis mit dem Betroffenen haben.
- Auftragsdatenverarbeiter (gemäß § 11 BDSG), die personenbezogene Daten im Rahmen von Dienstleistungen verarbeiten (und zumindest für diesen Teil nicht selbst meldepflichtig sind), nehmen de facto in vielen Fällen für ihre zur Meldung verpflichteten, aber inhaltlich überforderten Auftraggeber diese Verpflichtung stellvertretend wahr.
- Unabhängig von der Größe des Unternehmens und der Anzahl der mit der Verarbeitung personenbezogener Daten beschäftigter Personen sind Unternehmen zur Meldung verpflichtet, wenn geschäftsmäßig zu Zwecken der Übermittlung, auch der anonymisierten Übermittlung, verarbeitet wird. Diese Unternehmen müssen schon heute wie auch nach der Anhebung des Schwellenwertes entweder an die Aufsichtsbehörde melden oder einen bDSB berufen.
- Unabhängig von der Größe des Unternehmens und der Anzahl der mit der Verarbeitung personenbezogener Daten beschäftigter Personen sind Unternehmen zur Durchführung einer Vorabkontrolle verpflichtet, wenn sie Verarbeitungen durchführen, von denen besondere Gefährdungen für das Persönlichkeitsrecht der Betroffenen ausgehen. Dies ist insbesondere erfüllt, wenn besondere Arten personenbezogener Daten gemäß § 3 Abs. 9 BDSG verarbeitet werden. Es ist davon auszugehen, dass Ärzte, Apotheken, Rechts-

anwälte und Steuerberater regelmäßig derartige, besonders sensible Daten verarbeiten und daher eine Vorabkontrolle durchführen müssen, soweit sie, was in der Regel anzunehmen ist, die Daten Dritter verarbeiten, die mit ihnen in keinem Vertragsverhältnis stehen (z. B. Daten über Familienangehörige des Patienten, die ein Arzt im Rahmen einer Anamnese erhebt). Da diese Vorabkontrolle jedoch vom betrieblichen Datenschutzbeauftragten durchzuführen ist, ergibt sich die Pflicht zu dessen Bestellung hieraus automatisch. Es erscheint unverständlich, warum dies in der Begründung zum Gesetzentwurf zwar ausdrücklich erwähnt wird (um zu »belegen«, dass die Betroffenenrechte nicht verkürzt würden), ausgerechnet jedoch Arztpraxen, Apotheken, Rechtsanwalts- und Steuerberaterkanzleien als Beispiele für die überzogene (und daher abzuschaffende) Meldepflicht/Bestellungspflicht aufgeführt werden. Dass den unzutreffenden Auffassungen berufsständischer Lobbys (wie z.B. der Bundesärztekammer) gefolgt wird, Arztpraxen, Anwaltskanzleien u.ä. wären von der Pflicht zur Vorabkontrolle ausgenommen, lässt vermuten, dass die Verfasser der Begründung mit der tatsächlichen Lage in der Praxis nur wenig vertraut sind.

B. Die Darstellung erweckt außerdem hinsichtlich des bei den zur Meldung verpflichteten, kleineren Unternehmen erforderlichen Aufwandes einen vollkommen falschen Eindruck, der dem in der Praxis tatsächlich entstehenden Aufwand in keiner Weise entspricht. Auch kleine Unternehmen erstellen schon aus Eigeninteresse und zur ordnungsgemäßen Organisation ihrer EDV grundlegende Dokumentationen. Diese reichen in aller Regel als Grundlage für die Zusammenstellung der Meldeangaben gemäß § 4 e BDSG vollkommen aus, so dass nur wenig zusätzlicher personeller und zeitlicher Aufwand entsteht. Der Grundaufwand für die Erstellung einer ordnungsgemäßen Dokumentation lässt sich jedoch – schon im Eigeninteresse – nicht reduzieren, auch nicht durch den Wegfall der Meldepflicht.

Fazit: Deutlich weniger kleine Unternehmen als dargestellt werden durch die Anhebung des Schwellenwertes von der Meldepflicht/Bestellungspflicht befreit.

Daher ist eine wesentliche Entlastung verantwortlicher Stellen durch die entfallende Meldepflicht nicht zu erwarten.



Zu 2. – Entlastung der Aufsichtsbehörden

Es wird ausgeführt, dass die nach Landesrecht zuständigen Aufsichtsbehörden für die Kontrolle der Durchführung des Datenschutzes im nicht-öffentlichen Bereich Einsparungen auf Grund der zurückgehenden Zahl von Meldungen nach § 4d BDSG erzielen könnten.

Tatsächlich ist heute schon zu beklagen, dass die Aufsichtsbehörden wegen der geringen zur Verfügung stehenden Kapazitäten nur sehr eingeschränkt ihrer Aufsichtsfunktion nachkommen können.

Unternehmen aller Größenordnungen müssen nur mit einer extrem geringen Wahrscheinlichkeit mit einer Überprüfung rechnen. Bereits in der derzeitigen Situation ist daher zu bezweifeln, dass Datenschutzverletzungen im nicht-öffentlichen Bereich aufgedeckt, geschweige denn angemessen geahndet werden können.

Gleichzeitig sind die Melderegister der Aufsichtsbehörden fast leer, die sich aus den Meldeangaben kleiner Unternehmen ohne Pflicht zur Bestellung eines bDSB speisen sollten. Die Praxis lehrt, dass der Pflicht zur Abgabe der Meldeangaben meist aus Unkenntnis oder Unwilligkeit nicht nachgekommen wird. Obwohl die Aufsichtsbehörden diesem Missstand durch verstärkte Kontrollen abhelfen müssten, sind sie dazu aus Kapazitätsgründen ebenfalls nicht in der Lage. Da die Führung der Melderegister also bereits heute kaum Aufwand für die Aufsichtsbehörden mit sich bringt, kann eine Entlastung durch weniger meldepflichtige Unternehmen schlechterdings nicht erzielt werden.

Eine Erhöhung der Anzahl nicht-öffentlicher Stellen, die keiner anderen als der Datenschutzaufsicht der Aufsichtsbehörden unterstehen, würde die beschriebenen Missstände weiter zu Ungunsten der Betroffenen verschärfen und eine zusätzliche qualitative Verschlechterung des Datenschutzniveaus im nicht-öffentlichen Bereich nach sich ziehen. Die ohnehin überforderten Aufsichtsbehörden können noch mehr Unternehmen nicht kontrollieren, so dass diese de facto dann überhaupt keiner wirksamen Datenschutzaufsicht mehr unterstehen.

Fazit: Die angenommene Entlastung der Aufsichtsbehörden ist nicht anzunehmen. Vielmehr ist mit einer Mehrbelastung durch eine Zunahme der dann in die Zuständigkeit der Aufsichtsbehörden fallenden Kleinunternehmen ohne eigenen betrieblichen Datenschutzbeauftragten zu rechnen.

Zu 3. – Beseitigung der Unklarheiten einer komplizierten Regelung

Es wird angeführt, dass »die komplizierte Regelung des Bundesdatenschutzgesetzes in den betroffenen Betrieben und Unternehmen nicht selten zu Unklarheiten bei der Beachtung der Meldepflicht und der Pflicht zur Bestel-

lung eines betrieblichen Datenschutzbeauftragten geführt« habe.

Inwieweit hiermit speziell die Regelung zur Bestellung eines betrieblichen Datenschutzbeauftragten oder die Gesamtheit der im BDSG festgeschriebenen Regelungen gemeint ist, wird nicht näher ausgeführt.

Unabhängig vom Bezug der Kritik ist jedoch bemerkenswert, dass die komplizierte Anwendung eines Gesetzes nicht etwa durch eine Novellierung mit eindeutigeren Regelungen ersetzt, sondern schlicht die Zahl der Normadressaten gesenkt werden soll. Gerade so als würde man in einem Haus mit defekter Heizung nicht etwa die Heizung reparieren, sondern einem Teil der Mieter kündigen.

Es stellt sich in diesem Zusammenhang erneut die Frage, warum noch immer keine Schritte zur lange angekündigten und überfälligen Modernisierung des Datenschutzrechts ergriffen wurden und statt dessen wiederum nur Flickschusterei betrieben wird.

Fazit: Die geplante Herausnahme von kleinen und mittleren Unternehmen aus dem System der betrieblichen Selbstkontrolle ist nicht geeignet, die Regelungen des Bundesdatenschutzgesetzes zu vereinfachen. Die vorgeschlagene Änderung trägt nicht zur Beseitigung von Unklarheiten bei.

Zu 4. – Entbürokratisierung

Es wird angeführt, dass durch das Entfallen der Pflicht zur Bestellung eines betrieblichen Datenschutzbeauftragten ein Beitrag zur Entbürokratisierung geleistet werde.

Vordergründig müssten gemäß der vorgeschlagenen Regelung Betriebe, die weniger als 20 Personen mit der automatisierten Verarbeitung personenbezogener Daten beschäftigen, die Funktion des betrieblichen Datenschutzbeauftragten nicht mehr besetzen. Tatsächlich kommen auf diese Betriebe jedoch in großer Zahl zusätzliche bürokratische Anforderungen zu. Dann nämlich, wenn in den unter 1. aufgeführten Fällen eine Meldepflicht an die Aufsichtsbehörde besteht, wird für diese Unternehmen der bürokratische Aufwand, einer externen Stelle (der Meldebehörde) die erforderlichen Dokumentationen in der jeweils aktuellen Version zur Verfügung zu stellen, wesentlich höher sein als wenn die Lieferung an den internen bDSB zu erfolgen hätte. Da die unter 1. genannten Fälle (trotz Schwellenwert zur Meldung verpflichtete Unternehmen) voraussichtlich sehr häufig sein dürften, ist eine entbürokratisierende Wirkung nicht zu erwarten.

Fazit: Die vorgeschlagene Gesetzesänderung führt keinesfalls zu geringerer bürokratischer Belastung der Unternehmen. Vielmehr ist in einer Vielzahl der Fälle mit einer Komplizierung betrieblicher Prozesse durch die nötige Einbeziehung der (externen) Aufsichtsbehörden in die für den Datenschutz relevanten Abläufe zu befürchten.

Zu 5. – Senkung der Kosten in den Betrieben

Die vorgeschlagene Gesetzesänderung soll zu einer Senkung der Kosten in den Betrieben führen, ohne dass dies näher erläutert oder begründet würde.

Wie bereits dargelegt, wird ein nicht unerheblicher Teil der von der Änderung betroffenen Betriebe nach wie vor einen betrieblichen Datenschutzbeauftragten bestellen, bzw. die Meldung der eingesetzten Verfahren an die zuständige Aufsichtsbehörde vornehmen müssen.

Die Erfüllung gesetzlicher Datenschutz-Anforderungen (von der die Bestellung eines bDSB ja nur eine ist) durch jedes Unternehmen ist nicht an die Zahl der Mitarbeiter geknüpft, sondern einzig und allein an die Tatsache der Verarbeitung personenbezogener Daten. Daher sind im Falle eines nicht verfügbaren (weil nicht bestellten) Datenschutzbeauftragten die Prüfung der Zulässigkeit von Erhebung, Verarbeitung und Nutzung, die Kommunikation mit der Aufsichtsbehörde, die Auskunftserteilung an Betroffene, die evtl. nötige Erstellung des Verfahrensverzeichnisses und alle anderen Datenschutzaufgaben künftig von der Geschäftsleitung selbst vorzunehmen – eine für Nicht-Fachleute aufwändige Pflicht. Es ist zu befürchten, dass durch die Notwendigkeit der Beschäftigung fachfremder Mitarbeiter mit Datenschutzthemen durch die zu erwartende ineffizientere Aufgabenbewältigung eher höhere Kosten für die betroffenen Betriebe entstehen als wenn sich ein fachkundiger Datenschutzbeauftragter mit deren Erledigung befasst hätte.

Fazit: Statt einer prognostizierten Senkung der Kosten in den betroffenen Betrieben ist wegen der Befassung fachfremden Personals mit der Umsetzung von Datenschutz-Anforderungen eher mit höheren Kosten, jedenfalls aber mit einer Verschlechterung des Datenschutzniveaus zu rechnen.

Zu 6. – Stärkung der Eigenverantwortung der Betriebe

Es wird behauptet, dass die vorgeschlagene Gesetzesänderung die Eigenverantwortung der Betriebe stärken würde, ohne dass dies näher erläutert oder ausgeführt würde.

Das Modell der innerbetrieblichen Selbstkontrolle durch betriebliche Datenschutzbeauftragte wird zu Recht immer wieder, zunehmend auch im Ausland, als effizientes Gegenmodell zu einer staatlich geführten Fremdkontrolle gelobt. Gerade die Präsenz des fachkundigen Datenschutzbeauftragten im eigenen Hause hat den Schutz der Persönlichkeitsrechte einerseits und die Stärkung der betrieblichen Eigenverantwortung andererseits befördert.

Inwiefern nun ausgerechnet die Abschaffung dieses internen Beauftragten und die Einführung der Fremdkontrolle durch die Aufsichtsbehörde die Eigenverantwortung der Betriebe stärken soll, bleibt das Geheimnis der Autoren des Gesetzesvorschlags.

Fazit: Zur angenommenen Stärkung der Eigenverantwortung der Betriebe verhält sich der Gesetzentwurf geradezu kontraproduktiv. Er würde vielmehr eine Schwächung der Eigenverantwortung der Betriebe hervorrufen, da er innerbetriebliche Selbstkontrolle durch Fremdkontrolle ersetzt.

Umfrage

Bürger für Fußball-Videoüberwachung

Auf die Frage »Sind Sie für Videoüberwachung von öffentlichen Plätzen im Rahmen der Fußball-Weltmeisterschaft« antworteten von rund 1000 Befragten am 20./21.02.2006 dem Marktforschungsinstitut im Auftrag des Spiegels mit »ja« 84 % und mit »nein« 13 % (Der Spiegel 9/2006, 20).

DATENSCHUTZ NACHRICHTEN

REGISTER FÜR DEN JAHRGANG 2005

Bearbeitung: Karin Bauer

Register-Inhalt

I. Themenschwerpunkte der einzelnen Ausgaben

II. Aufsätze

III. Stellungnahmen, Aufrufe, Presseerklärungen

IV. Rechtsprechung

V. Buch- und Broschürenbesprechung

VI. Deutsche Datenschutznachrichten

Baden-Württemberg

Bayern

Berlin

Brandenburg

Bund

VII. Ausländische Datenschutznachrichten

Israel

Italien

Japan

Niederlande

Österreich

Russland

Schweden

Schweiz

Spanien

Südkorea

Türkei

UNO

USA

Vatikan

Vereinigte Arabische Emirate

VIII. Welt der Technik

IX. Welt der Gentechnik

X. Stichworte

Datenschutz Nachrichten – Jahresregister 2005
Herausgegeben von der Deutschen Vereinigung für Datenschutz e.V. – DVD
Geschäftsstelle: Bonner Talweg 33-35, 53113 Bonn, Tel. 0228-222498, E-Mail: dana@datenschutzverein.de
Bearbeiterin: Karin Bauer — Beilage zur DANA 1/2006

Datenschutznachrichten

Deutsche Datenschutznachrichten

Bund

PKG neu besetzt

Der Deutsche Bundestag hat das Parlamentarische Kontrollgremium (PGK), dem die Kontrolle der deutschen Geheimdienste obliegt, mit neun männlichen Abgeordneten neu besetzt. Das Gremium wird zu Beginn jeder Legislaturperiode neu gebildet. Alle von den Fraktionen vorgeschlagenen Kandidaten wurden bestätigt, auch der Abgeordnete der Linken-Fraktion, Wolfgang Neskovic. Neskovic hat eine schillernde Vergangenheit hinter sich beim Arbeitskreis sozialdemokratischer Juristinnen und Juristen (ASJ) und später bei Bündnis 90/Die Grünen. Seit drei Jahren ist er Richter am Bundesgerichtshof; er ist parteilos, also weder bei der PDS noch bei der WASG. Als Vorsitzender Richter am Landgericht Lübeck hat der heute 57jährige 1992 von sich Reden gemacht, als er das »Recht auf Rausch« proklamierte und forderte, dass Alkohol und Haschisch gleich behandelt werden müssten. Das Bundesverfassungsgericht hat ihm, den Unionsländer deswegen für »verrückt« erklärt hatten, insofern weitgehend Recht gegeben.

Für die Unionsfraktion wurden Norbert Röttgen, Bernd Schmidbauer und Hans-Peter Uhl in das PKG gewählt. Schmidbauer war unter Helmut Kohl Geheimdienstkoordinator im Kanzleramt. Die SPD entsendet Olaf Scholz, Joachim Stünker und Fritz Rudolf Körper. Die Oppositionsparteien sind neben Neskovic mit Max Stadler (FDP) und Hans-Christian Ströbele (Bündnis 90/Grüne) vertreten. Schmidbauer und Ströbele sind die einzigen aus dem alten PKG, die bleiben. Bei Ströbeles Wahl im Jahr 1999 hatte es noch große Vorbehalte gegeben; beim ersten Wahldurchgang war er durchgefallen und schaffte es erst beim zweiten Anlauf. Bei der aktuellen Wahl bestand dagegen zwischen den Fraktionen große Einigkeit. Sogar die CDU hatte schon vor der Wahl signalisiert, dass im Interesse der Arbeitsfähigkeit des Gremiums die Mitglieder mit der erforderlichen Mehrheit gewählt werden müssten. Der frühere Vorsitzende Volker Neumann (SPD) ist als Abgeordneter ausgeschieden (SZ 15.12.2005, 7; Ramelsberger SZ 14.12.2005, 5).

Bund

Kommt doch noch der Geheimdienstbeauftragte?

Die jüngsten Geheimdienst-Skandale insbesondere um den Bundesnachrichtendienst (BND) haben zu einem Umdenken bei den politischen Parteien in Bezug auf die Geheimdienstkontrolle geführt: Die wichtigen Dinge über die Geheimdienste erfuhren die Mitglieder des Parlamentarischen Kontrollgremiums (PKG) alle aus der Zeitung und nicht von den Diensten direkt während der hochgeheimen PKG-Sitzungen: geheime CIA-Flüge, nach Afghanistan verschleppte Deutsche, vom BND bespitzelte Journalisten. Partei übergreifend fordern die parlamentarischen Kontrolleure, den »zahnlosen Tiger« PKG, so der Grünen-Abgeordnete Christian Ströbele, durch einen ordentlichen Wachhund zu ersetzen.

Der CSU-Abgeordnete Hans-Peter Uhl, neu im PKG (s.o.), fordert, dem Gremium Rechte wie einem Untersuchungsausschuss zu geben, so dass Zeugen vernommen und Akten eingesehen werden können. Und der innenpolitische Sprecher der CDU Wolfgang Bosbach meint: »Wir müssen sicherstellen, dass die Mitglieder des Kontrollgremiums nicht nur das erfahren, was sie erfahren sollen, sondern das, was sie erfahren müssen.« Sein SPD-Kollege Dieter Wiefelspütz sinnierte darüber, dass nicht alles, was als geheim deklariert wird, auch geheim sei: »Man könnte vieles öffentlich machen, ohne dass die Arbeit der Dienste auch nur einen Millimeter eingeschränkt wird.« Christian Ströbele fordert einen Geheimdienstbeauftragten, der wie der Datenschutzbeauftragte die Dienste nach Dunkelstellen durchkämmen soll. Dieser soll unabhängig sein und vom Parlament gewählt. Wolfgang Neskovic von der Linken-Fraktion wünscht sich Mitarbeiter, die sich in den Geheimdiensten auskennen. Er möchte, dass sich das PKG jederzeit in einen Untersuchungsausschuss umwandeln kann.

Die Parlamentarier erhalten teilweise Unterstützung aus dem Dienstebereich. Hansjörg Geiger, der Präsident des Bundesamtes für Verfassungsschutz (BfV) und des BND war, fordert einen »ernst zu nehmenden Counterpart« für die Dienste. Ihm schwebt ein Geheimdienstkontrolleur mit eigener Dienststelle vor: »Die Kontrolle funktioniert grundsätzlich nicht, also nützt es nichts, nur einige Stellschrauben anzuziehen. Man muss die Kontrolle dem Parteienstreit entheben und echte Fachleute einsetzen, die auch Zeit haben, sich darum zu kümmern.« Die bisherige Kontrolle der Dienste ist zersplittert. Es gibt den G-10-Ausschuss, der ursprünglich und weiterhin vor allem Telefonüberwachungen kontrolliert, einen Untersuchungsausschuss der Haushälter, der die Kosten von Geheimdienst-Operationen begutachtet und das PKG. Außerdem sind auch zuständig der Rechnungshof und der Bundesbeauftragte für den Datenschutz und Informationsfreiheit (BfDI). Geiger fordert, die geheimdienstspezifischen Organe unter dem Dach eines Geheimdienstbeauftragten zusammenzuführen. Dabei findet er die Unterstützung von Hermann Bachmaier (SPD), der von 1983 bis 2005 Bundestagsabgeordneter war und sechs Jahre lang Mitglied im PKG: »Ich wäre für einen Vorschlag, den neben dem vor kurzem ausgeschiedenen Justiz-Staatssekretär Hansjörg Geiger Peter Struck, Otto Schily und ich schon vor Jahren gemacht haben: einen Geheimdienst-Beauftragten mit umfassenden Informations- und Zugangsrechten zu installieren, der als eine Art Hilfsorgan des Bundestags fungiert und dem Parlament verantwortlich ist. Der hätte sicher Einiges zu tun.«

Einen anderen, erheblich unrealisti-

scheren und weniger effektiven Vorschlag verfolgt ein anderer früherer BfV-Präsident: Eckart Werthebach. Er setzt darauf, die Präsidenten der Dienste stärker in die Pflicht zu nehmen. Wenn sie die Parlamentarier zu wenig oder zu spät informierten, dann müsste das als Dienstvergehen gebrandmarkt werden und bis zur Entlassung aus dem Amt führen. Geigers Vorschlag wird von ihm abgelehnt; aus dem Geheimdienstbeauftragten könne schnell ein Parallel-Nachrichtendienst mit viel zu viel Bürokratie werden: »Dienste, die nicht kontrolliert werden wollen, können nur schwer kontrolliert werden.«

Das PKG hatte in den vergangenen Monaten zweimal hintereinander einen Sonderermittler eingesetzt. Der frühere Bundesrichter Gerhard Schäfer durchforstet für das PKG die Affäre um die BND-Bespitzelung von Journalisten. Die schärfste Waffe des PKG ist es, mit einer Zwei-Drittel-Mehrheit eine Kritik öffentlich zu machen. Hiervon haben sie im Herbst 2005 viermal hintereinander Gebrauch gemacht, so oft wie sonst in Jahren nicht (Ramelsberger SZ 05./06.01.2006; Ramelsberger/Roßmann SZ 18.01.2006, 5; Ramelsberger/Blechschmidt SZ 20.01.2006, 2; Der Spiegel 1/2006, 17).

Bund

Birthler weitere fünf Jahre Stasiakten-Beauftragte

Mit 486 Stimmen gegen 60 bei 17 Enthaltungen wurde die 58jährige Stasiakten-Beauftragte Marianne Birthler für weitere fünf Jahre in ihrem Amt bestätigt. Die frühere DDR-Bürgerrechtlerin war im Jahr 2000 zur Nachfolgerin von Joachim Gauck gewählt worden, der die Stasiakten-Behörde die ersten zehn Jahre nach ihrer Gründung geleitet hatte. Die erste Amtszeit Birthlers war bereits am 10.10.2005 zu Ende gegangen, doch musste die Wiederwahl wegen der Bundestagswahl 2005 verschoben werden. Kulturstaatsminister Bernd Neumann gratulierte: »Der fraktionsübergreifende Konsens im Deutschen Bundestag mit Ausnahme der Linkspartei hat das hohe Ansehen bestätigt, das die Stasiunterlagen-Behörde und ihre kompetente und engagierte Leiterin in der nationalen und internationalen Öffentlichkeit erworben hat.« Während Birthlers erster Amtszeit hatte vor allem der Rechtsstreit mit Altkanzler Helmut Kohl Aufsehen erregt (Dana 2/2002, S. 41). Die Behörde wurde am 03.10.1990 gegründet. Ihre Aufgabe ist die Erfassung, Erschließung, Verwaltung und Verwendung der Unterlagen des DDR-Ministeriums für Staatssicherheit. Dazu zählen etwa 180 Kilometer Akten, 1,3 Mio. Fotos und Dias, fast 5000 Filme und Videos, 164.000 Tonträger und etwa 20.000 Disketten und Magnetbänder (SZ 27.01.2006, 5, 4, vgl. von Bullion SZ 26.01.2006, 3).

Bund

Mobile Biometrie-Identifikation durch Polizei

Anfang 2006 begann das Bundeskriminalamt (BKA) mit seiner zweiten Phase des Pilotprojektes »Fast Identification«: In Streifenwagen der Polizei werden optische Fingerabdruck-Scanner (Fast-ID-Geräte) installiert, die einen direkten Datenabgleich der erfassten Daten mit dem zentralen Datenbestand des Automatisierten Fingerabdruck-Identifizierungs-Systems (AFIS) ermöglichen. In AFIS sind derzeit ca. 3,2 Mio. Fingerabdruck-Datensätze digital gespeichert. Bislang konnten die Beamten bei der Nutzung von mobilen Fingerabdruck-Scannern nur auf einen lokalen Datenbestand zugreifen, der allerdings auch bis zu 50.000 Datensätze von definierten Zielgruppen umfassen konnte. Die per Fast-ID-Gerät erfassten Abdrücke – linker und rechter Zeigefinger – werden drahtlos an AFIS übermittelt, wo sie in ein beschleunigtes Identifizierungsverfahren gelangen. Stellt das System eine Fingerrillen-Übereinstimmung fest, so wird nach einer Überprüfung durch einen Daktyloskopen dies als Treffer direkt zurück an die Einsatzkräfte gemeldet.

Die neue Technik müsse sich, so das BKA, bei der Treffergenauigkeit als auch im Antwort-Zeit-Verhalten bewähren. Sie soll dann nicht nur im täglichen Streifendienst, sondern auch bei Sonder- und Großveranstaltungen wie der Fußball-WM eingesetzt werden. Die Erprobung der Technik erfolgte zunächst in enger Zusammenarbeit mit der bayerischen Polizei mit den dort bereits vorhandenen »Car-PC-Systemen«. Laut einer öffentlichen Ausschreibung befinden sich bei der bayerischen Polizei derzeit 365 Car-PCs im Einsatz; 100 sollen hinzukommen. Ab Februar 2006 folgt dann die Testung auch durch die Bundespolizei am Flughafen Frankfurt/Main. Die in der ersten Phase noch beteiligten Polizeibehörden von Hessen und Rheinland-Pfalz nehmen laut BKA nicht mehr teil. BKA-Präsident Jörg Zierke ist begeistert: »Die mobile Anbindung von Fast-ID-Geräten an das zentrale AFIS stellt einen weiteren Baustein in dem Bestreben der Polizei dar, höchstmögliche Sicherheit für die Allgemeinheit bei möglichst geringer Beeinträchtigung des Bürgers zu gewährleisten« (www.heise.de 11.01.2006).

Bund

CDU-CSU-Landespolitiker fordern Fußfessel für Ausländer

Der niedersächsische Innenminister Uwe Schünemann (CDU) fordert elektronische Fußfesseln für radikale Islamisten: »Damit lassen sich viele der etwa 3000 gewaltbereiten Islamisten in Deutschland, Hassprediger und in ausländischen Terrorcamps ausgebildete Kämpfer überwachen.« Die Regelung hierzu könne ohne verfassungsrechtliche Bedenken ins Ausländergesetz aufgenommen werden. Die elektronische Fußfessel sei für die gewaltbereiten Islamisten geeignet, die wegen drohender Folter nicht in ihre Heimat abgeschoben werden können. Sie dürften sich dann nur noch in bestimmten Gebieten aufhalten: »Das bedeutet auf jeden Fall mehr Sicherheit.« Die Innenministerkonferenz soll nach seinem Willen im Frühjahr 2006 die Fußfessel beschließen. Bisher wird das Instrument nur bei verurteilten Straftätern eingesetzt. Nordrhein-Westfalens Innenminister Ingo Wolf (FDP) lehnt Schünemanns Vorschlag ab. Der Vorstoß sei rechtsstaatlich hoch bedenklich: »Ich empfehle Herrn Schünemann dringend einen Blick in unser Grundgesetz. Das Ausländerrecht ist in keinem Fall der richtige Platz für die Verankerung einer Islamisten-Fußfessel«.

Auch Bayerns Innenminister Günther Beckstein (CSU) fordert eine weitere Verschärfung des Aufenthaltsgesetzes. Gefährliche Ausländer, die nicht abgeschoben werden können, sollten nach seiner Ansicht in Haft genommen oder zumindest mit einer

»elektronischen Fußfessel« versehen werden. Beckstein beklagte, hier gebe es eine »äußerst unbefriedigende Lücke«. Ein Ausländer, der von den Sicherheitsbehörden als besonders gefährlich eingestuft werde und dessen Ausweisung gerichtlich bestätigt sei, könne nicht in seine Heimat abgeschoben werden, wenn ihm dort Folter oder die Todesstrafe drohe. »Dann läuft er in Deutschland als freier Mann herum. Das halte ich für einen unerträglichen Zustand.« Mit der Drohung von Haft und Fußfessel »bringen wir solche Leute dazu, freiwillig auszureisen«.

Die Vorsitzende des Bundestagsausschusses für Menschenrechte, Herta Däubler-Gmelin (SPD), entgegnete, man könne nicht gegen Folter und Todesstrafe sein und gleichzeitig Menschen in Länder ausliefern, in denen beides »gang und gäbe« sei. Die Forderung nach der Fußfessel verstoße gegen den Grundsatz der Unschuldsvermutung. Der Parlamentarische Geschäftsführer der Grünen-Fraktion Volker Beck hielt dem CSU-Politiker vor, seine Vorschläge seien »im Kern rassistisch«. Das zeige schon die Unterscheidung in gefährliche Ausländer und gefährliche Deutsche, denen Beckstein offenbar keine Fußfessel anlegen wolle (SZ 29.12.2005, 4, 6; SZ 16.01.2006, 6).

Bund
Fotos im Ausländerzentralregister u.v.m.

Die Bundesregierung will das Ausländerrecht in wichtigen Punkten verschärfen, um dadurch Zwangsehen, Prostitution und Schleusung zu erschweren. Ein 260seitiger Gesetzentwurf des Bundesinnenministeriums sieht u.a. ausdrücklich vor, dass Aufenthaltserlaubnisse bei Scheinehen verboten werden; der Familiennachzug von Ehepartnern wird erst ab dem 21. Lebensjahr erlaubt. Jeder Ausländer soll »auf Verlangen« ein digitales Foto vorlegen, das im Ausländerzentralregister (AZR) gespeichert werden darf. Langfristig will das Ministerium so bis zu 30 Mio. Lichtbilder erfassen. In dem Register können die Ausländerbehörden künftig bei Zweifeln an der Identität eines Antragstellers mittels biometrischer Merkmale recherchieren. Für Polizei und Justizbehörden ist ein Online-Zugang vorgesehen. Formaler Hintergrund ist für Berlin die Umsetzung von 11 EU-Richtlinien, mit denen die »zentralen Elemente« des Ausländer- und Asylrechts in der Gemeinschaft angeglichen werden sollen. Das Gesetz soll spätestens im Juli 2006 in Kraft treten (Der Spiegel 2/2006, 18).

Bund
Behördliche Vaterschaftsanfechtung bei »Scheinvätern«

Nach der Bekämpfung der Scheinehen nun die Bekämpfung der Scheinväter: Ausländern soll es künftig schwerer gemacht werden, durch falsche Vaterschaftsanerkennung ein Aufenthaltsrecht zu erschleichen. Auch die Erschleichung von Sozialleistungen per Scheinvaterschaft soll erschwert werden. In Berlin sollen angeblich an deutsche Sozialhilfeempfänger bis zu 10.000 Euro für die falsche Anerkennung von Vaterschaften gezahlt werden. Da die Sozialhilfe-Empfänger keinen Unterhalt leisten können, muss anschließend der Staat die Kosten für Frau und Kinder übernehmen.

Über die Justizministerkonferenz Ende November 2005 setzte sich das Land Bayern dafür ein, dass Behörden zweifelhafte Vaterschaften anfechten können, z.B. – so die bayerische Justizministerin Beate Merk (CSU) – wenn »der Anerkennende nicht mit der Mutter und dem Kind in einem sozialen Familienverbund zusammenlebt oder auch sonst nicht bereit ist, für das Kind zu sorgen. Nach dem jetzigen Recht dürfen nur die Eltern und das Kind selbst die Vaterschaft anfechten. Ausländerbehörden hatten entdeckt, dass bundesweit in rund 2.000 Fällen zwischen April 2003 und April 2004 ausreisepflichtige Ausländer die Vaterschaft für ein deutsches oder ein ausländisches Kind mit Aufenthaltsgenehmigung anerkannten. Nach einer Umfrage teilte die bayerische Justizministerin Beate Merk (CSU) mit, dass von April 2003 bis April 2004 bundesweit 1.920 ausländische Männer ohne Aufenthaltsgenehmigung die Vaterschaft eines deutschen Kindes anerkannt hätten. Außerdem wurde 2.289 ausländischen Müttern ein Bleiberecht zugestanden, weil der Vater ihres Kindes Deutscher sei. 73% dieser Frauen seien ausreisepflichtig gewesen, als die Vaterschaft anerkannt wurde.

Justizministerin Zypries schloss sich der Initiative an. Auch sie will über eine Änderung des Bürgerlichen Gesetzbuches die Möglichkeit eröffnen, umstrittene Vaterschaften zu überprüfen. Die Grünen verurteilten die geplante Neuregelung. Deren Bundestagsabgeordneter Josef Winkler meinte, das Anfechtungsrecht stelle alle Familien mit einem ausländischen Elternteil ohne sicheren Aufenthaltsstatus unter Generalverdacht. Man müsse sich fragen, ob die Zahl der Verdachtsfälle wirklich einen so schwerwiegenden Eingriff rechtfertige. Auch der Deutsche Anwaltsverein (DAV) lehnt die Verschärfung ab, so Susanne Schröder, Vorsitzende der Arbeitsgemeinschaft Ausländer- und Asylrecht im DAV: »Wenn zwei Menschen entscheiden, gemeinsame Eltern eines Kindes zu sein, haben das staatliche Behörden zu akzeptieren« (Der Spiegel 46/2005, 20; Roßmann SZ 18.11.2005, 5).

Bund
Praxis des Kontoevidenzverfahrens mangelhaft

Seit April 2005 hat die Finanzverwaltung das Recht, die Daten der 500 Millionen bei Banken in Deutschland geführten Konten und Depots abzufragen. Auch Sozialbehörden können ohne Anfangsverdacht einer Straftat die Stammdaten der Konteninhaber – Name, Geburtsdatum, Anschrift, Zahl der Konten bei welchen Kreditinstituten – einsehen (vgl. DANA 1/2005, 18 f., 2/2005, 36, 47 f.). Bei einer vom Bundesbeauftragten für den Datenschutz und Informationsfreiheit veranlassten Stichprobe in drei nordrhein-westfälischen Finanzämtern stellte sich heraus, dass neun von zehn Kontenabfragen Mängel aufwiesen. So waren z.B. die betroffenen Steuerzahler nicht vorher zum Sachverhalt befragt oder die Kontenschnüffelei nicht lückenlos dokumentiert worden.

Nach einer Umfrage des Genossenschaftsverbandes Bayern (GVB) hat das Kontoevidenzverfahren zu einer Kapitalflucht »sauberen Geldes« von hochgerechnet rund 2 Milliarden Euro geführt. Vor allem österreichische Banken profitierten. Dort wird das »Bankgeheimnis« ähnlich streng gehütet wie in der Schweiz. Von Kapitalerträgen werden anonym 15 % Quellensteuer abgeführt. Das Alpenland beteiligt sich auch nicht an der neuen EU-Regelung, wo-

nach Zinseinkommen von Ausländern den Heimatfinanzämtern automatisch mitgeteilt werden. Inzwischen locken die Österreicher auch kleine Anleger mit dem Versprechen, ihr Vermögen vor Hartz IV zu sichern (Der Spiegel 1/2006, 63).

Bund

Mit Kuno gegen EC-Kartenbetrug

Auf der Innenministerkonferenz im Dezember 2005 in Karlsruhe wurde den Ländern empfohlen, sich an einem Verfahren zur Eindämmung des Missbrauchs gestohlener EC-Karten zu beteiligen. Dieses war zuvor unter dem Namen »Kuno« in Dresden erprobt worden. Mit dem Einzelhandel wurde die Einrichtung einer zentralen in Stuttgart eingerichteten Sperrdatei vereinbart. Die Daten werden den Händlern zur Verfügung gestellt, die damit erkennen können, wenn ein Dieb mit einer gestohlenen Karte ohne PIN einkaufen will. Nordrhein-Westfalens Innenminister Ingo Wolf (FDP) verspricht sich von der Einführung des Systems einen »Quantensprung« bei der Bekämpfung von EC- und Kreditkartenbetrug. In Dresden hatte sich die Schadensumme für den Einzelhandel durch gestohlene EC-Karten nach Einführung von Kuno halbiert. Bundesweit stieg dagegen die Zahl der Karten- und Scheckdiebstähle im Jahr 2004 um 8,9% auf 111.254 Fälle an, was dem Handel einen Schaden von ca. 54 Mio. Euro verursachte (Eckernförder Ztg. 10.12.2005, 8; Der Spiegel 49/2005, 20).

Bund

Rechnungshof fordert Sozialdatenabgleich

Der Bundesrechnungshof hat die Bundesagentur für Arbeit (BA) scharf angegriffen, weil sie bei der Verfolgung von Sozialleistungsmissbrauch in tausenden von Fällen den Abgleich von Daten verweigert habe. Ein Sprecher des Arbeitsministeriums wies die Vorwürfe zurück: »Für den verlangten massenhaften Datenabgleich gibt es keine rechtliche Grundlage.« Dies sei auch die Auffassung des Bundesbeauftragten für den Datenschutz. Allenfalls bei einem konkreten Anfangsverdacht könne die BA handeln. Damit geht der Grundsatzstreit um Datenschutz und Sozialleistungsmissbrauch in die nächste Runde. Das Land Baden-Württemberg hat im Dezember 2005 einen Entschließungsantrag in den Bundesrat eingebracht, der auf eine gesetzliche Ausweitung des Austauschs von Daten zwischen Ermittlungsbehörden und Sozialbehörden zielt. Dabei verweist die Stuttgarter CDU-FDP-Regierung ausdrücklich auf den Fall, der Anlass der nun bekannt gewordenen Rüge des Rechnungshofes ist.

Die Staatsanwaltschaft Frankfurt hatte schon im Jahr 2000 bei einem Steuerstrafverfahren gegen Kunden der türkischen Nationalbank deren Daten sichergestellt. Viele der in Deutschland lebenden Ausländer, so die Vermutung der Ermittler, beziehen trotz Vermögens Sozialleistungen. Sie gaben das Material an das Hauptzollamt Stuttgart als Teil der Finanzverwaltung, welche von der Bundesagentur 2004 einen Datenabgleich forderte. Diese verweigerte sich unter Hinweis auf den Datenschutz, so ein BA-Sprecher: »Wir hätten da 20.0000 türkischen Bankkunden unter Pauschalverdacht stellen müssen.« Im Bundesrechnungshof wird inzwischen eingeräumt, es gebe ein gesetzliches Problem bei der Datenweitergabe. Auf Unverständnis stoße aber weiterhin, dass die BA nicht eigene Ermittlungen aufgenommen habe (SZ 24.12.2005, 6).

Bund

Gesundheits-Pflichtuntersuchung bei Kleinkindern geplant

Nach dem Saarland fordern nun auch andere Bundesländer, die Pflicht zur ärztlichen Untersuchung von kleinen Kindern gesetzlich zu verankern. Eine entsprechende Gesetzesinitiative soll, so die Hamburger Bürgerschaft, so schnell wie möglich im Bundesrat eingebracht werden. Nach dem qualvollen Hungertod der kleinen Jessica vor knapp einem Jahr und weiteren Fällen von vernachlässigten Kindern in Hamburg sollten so Wiederholungen verhindert werden. Nach den Vorstellungen des Hamburger Gesundheitssenators Jörg Dräger (parteilos) sollen Eltern, die ihr Kind nicht untersuchen lassen wollen, an die Behörden, vorzugsweise an das Jugendamt gemeldet werden: »Es geht darum, dass die Ämter anders als bisher überhaupt informiert werden dürfen.« Diese könnten die Eltern dann vorladen. Außerdem soll ein Informationsaustausch zwischen Stellen wie Krankenkassen und Jugendämtern ermöglicht werden. Ein Bußgeld sei nicht geplant. Hamburg schließt sich damit einer Forderung des saarländischen Gesundheitsministers Josef Hecken (CDU) von Ende 2005 an. Auch die SPD hat bereits Unterstützung signalisiert. Generalsekretär Hubertus Heil hat sich Mitte Januar 2006 für Pflichtuntersuchungen ausgesprochen. Bundesfamilienministerin Ursula von der Leyen (CDU) lehnt eine solche Verpflichtung hingegen ab (SZ 19.01.2006, 6).

Bund

BKA nutzt Easy

Nach jahrelangen Fehlschlägen bei der Entwicklung eines eigenen Computerprogramms für die Fahndung probiert das Bundeskriminalamt (BKA) jetzt die Software Easy, die seit zwei Jahren erfolgreich im Bayerischen Landeskriminalamt bei der Ermittlung im Bereich Terrorismus und Organisierte Kriminalität genutzt wird. Easy ist eine Art »intelligente« Software, die den Datenbestand der Polizei durchforstet und dabei fall- und personenübergreifend nach Verbindungen sucht. Das Programm kann auch bei der Telekommunikationsüberwachung Verbindungsdaten analysieren und in Echtzeit Bewegungen eines Handy-Besitzers darstellen. Eine weitere Qualität des Programms liegt darin, dass es sämtliche Daten grafisch aufbereiten oder in Landkarten übertragen kann (Der Spiegel 51/2005, 20).

Bund

Abgeordneten-Nebeneinkünfte werden öffentlich

Von Anfang 2006 an müssen die Bundestagsabgeordneten ihre Einkünfte aus Nebentätigkeiten offenlegen. Gemäß einem vom Bundestag beschlossenen Verhaltenskodex müssen die Volksvertreter ihre Nebenjobs und die ungefähre Höhe der dabei erzielten Einkünfte im Handbuch des Parlaments veröffentlichen. Bisher genügte die Mittei-

lung an den Bundestagspräsidenten. Den Grünen und der Linkspartei reichen die neuen Offenlegungspflichten nicht; Union und FDP gehen sie zu weit. Der jetzige Bundestagspräsident Norbert Lammert (CDU) hatte zu Zeiten, als er noch Vizepräsident des Bundestages war, gemeint, die Anzeigepflichten der von der rot-grünen Koalition verabschiedeten Verhaltensregeln seien zu rigide und könnten Probleme verursachen. Diese Befürchtung habe er zwar »immer noch«, so heute Lammert, doch werde er die gefassten und nach der vorgezogenen Wahl vom neuen Bundestag übernommenen Regelungen anwenden: »Die Verhaltensrichtlinien sind beschlossen und in Kraft; wer sie ändern will, muss dazu Anträge stellen« (Der Spiegel 52/2005, 17).

Bund

Unternehmensdaten werden über Internet verfügbar

Ein am 14.12.2005 vom Bundeskabinett beschlossener Gesetzentwurf sieht vor, dass vom 01.01.2007 an alle wesentlichen publikationspflichtigen Daten von Unternehmen zentral über die Adresse www.unternehmensregister.de im Internet abgerufen werden können. Auch Handels-, Genossenschafts- und Partnerschaftsregister sollen dem gemäß spätestens bis zum 01.01.2007 auf elektronischen Betrieb umgestellt werden. Diese Maßnahmen würden, so Bundesjustizministerin Brigitte Zypries, »ganz erheblich dazu beitragen, den Wirtschaftsstandort Deutschland zu stärken. Alle wesentlichen offenlegungspflichtigen Unternehmensdaten wie Registereintragungen oder Jahresabschlüsse werden künftig online abrufbar sein. Anleger, Geschäftspartner und Verbraucher müssen sich die Informationen dann nicht mehr aus verschiedenen Datenbanken zusammensuchen, sondern können sie ohne nennenswerten Aufwand gebündelt über das Unternehmensregister im Internet abrufen.« Für die Veröffentlichung der Jahresabschlüsse sollen künftig nicht mehr die Amtsgerichte, sondern der elektronische Bundesanzeiger zuständig sein. Damit würde der »Bundesanzeiger zu einem zentralen Veröffentlichungsorgan für wirtschaftsrechtliche Bekanntmachungen aufgebaut.« Zuständig für die Führung von Handels-, Genossenschafts- und Partnerschaftsregister blieben dagegen die Amtsgerichte. Um die Verwaltung zu beschleunigen, könnten Unterlagen in Zukunft grundsätzlich nur noch elektronisch eingereicht werden. Die Bundesländer dürften allerdings Übergangsfristen vorsehen, nach denen die Unterlagen spätestens Ende 2009 auch noch in Papierform eingereicht werden können. Mit dem Gesetzesvorhaben werden nach Angaben des Bundesjustizministeriums zwei EU-Richtlinien sowie Beschlüsse der Regierungskommission Corporate Governance umgesetzt.

Beim Bundesamt der Deutschen Industrie (BDI) begrüßte Jan Wulfestange das Vorhaben: »Ziel ist, Informationen über Unternehmen allen schneller und kostengünstiger als bisher zugänglich zu machen. Aus unserer Sicht kann man das am besten über das Internet erreichen.« Die bisherige Veröffentlichungspflicht in Tageszeitungen sei im Vergleich dazu sehr mühsam, kosten- und zeitaufwändig gewesen. Möglicherweise bleibt diese Pflicht allerdings auch noch eine Weile bestehen, denn – so das Ministerium – »ob die Bekanntmachung für eine Übergangszeit darüber hinaus auch in Tageszeitungen erfolgen« müsse, könnten die Bundesländer in eigener Verantwortung regeln. Der Bundesverband Deutscher Zeitungsverleger kritisierte dagegen, der Gesetzentwurf sei ein »Schlag gegen die Interessen der Bürger und insbesondere der mittelständischen Wirtschaft.« Für die »große Mehrheit der Entscheider« seien Handelsregisteranzeigen in der Zeitung »auch im Fall der zusätzlichen Internet-Bekanntmachung unverzichtbar.« Auch Jürgen Kurz von der Deutschen Schutzvereinigung für Wertpapierbesitz sieht den Gesetzentwurf gespalten: »Natürlich ist mehr Transparenz zu begrüßen. Andererseits gibt es gerade viele Ältere, die keinen Internetanschluss haben. Wenn die Veröffentlichungspflicht in Tageszeitungen wegfällt, sind sie von wichtigen Informationen künftig ausgeschlossen« (SZ 15.12.2005, 22).

Bund

Kommt die PKW-Maut doch?

Die Koalitionspartner CDU/CSU und SPD haben entgegen ersten Äußerungen ihr klare Absage an die PKW-Maut aus ihrem Koalitionsvertrag gestrichen. Ursprünglich hatte es heißen sollen: »Eine Pkw-Maut lehnen wir ab.« Dieser Passus findet sich in der Schlussfassung des Vertrages nicht mehr. Zuvor hatten insbesondere die Bauindustrie darauf gedrungen, die Regierung möge sich in dieser Frage nicht vorzeitig festlegen. Vor allem im Zusammenhang mit einer Privatisierung von Autobahnen kann eine PKW-Maut interessant werden. Könnten die Autofahrer zur Kasse gebeten werden, könnte aus dem privaten Betrieb von Fernstraßen für Investoren ein Geschäftsmodell entstehen. Dabei bestünde das Risiko, dass der bei der LKW-Maut schon eingeführten überwachungsintensiven Form der Gebührenerhebung mit dem Verfahren von TollCollect auch für die PKW-Maut der Vorrang eingeräumt wird. Der designierte Verkehrsminister Wolfgang Tiefensee (SPD) lehnt aber bisher eine PKW-Maut ab: »Meine Haltung ist klar und unverändert: Für mich ist eine PKW-Maut kein Thema« (SZ 14.11.2005, 19).

Bund

Schäuble: Maut-Daten zur Strafverfolgung nutzen

Der neue Bundesinnenminister Wolfgang Schäuble setzt sich dafür ein, dass die beim LKW-Maut-Verfahren erhobenen Daten, die bisher einer strengen Zweckbindung unterliegen, für Strafverfolgungszwecke freizugeben. Er lässt eine entsprechende Gesetzesänderung prüfen. Anlass für diese Forderung ist die Tötung eines Parkplatzwächters, der von einem unerkannt entkommenden LKW überfahren worden ist. Der Vorschlag wurde vom Bund Deutscher Kriminalbeamter (BDK) unterstützt. Der Vorsitzende der CSU-Fraktion im bayerischen Landtag, Joachim Herrmann, wendet sich gegen Schäubles Vorschläge: Die LKW-Maut hätte ohne Datenschutz keine Mehrheit im Bundestag gefunden. Es könne nicht sein, dass der Datenschutz nachträglich ausgehöhlt werde. Die technische Überwachung gehe heute schon »weit über die 1984-Visionen von George Orwell« hinaus. Schäubles Vorschlag dürfe nicht dazu führen, dass jeder LKW auf Deutschlands Autobahnen potenzielles Fahndungsobjekt werde.

Kritisiert wurde der Schäuble-Vorschlag von allen Bundestags-Oppositi-

onsfraktionen: Grüne, FDP und Linkspartei. Unentschieden äußerte sich der Bundesbeauftragte für den Datenschutz, Peter Schaar: »Wenn tatsächlich der Nachweis geführt wird, dass diese Daten für die Verfolgung schwerster Straftaten erforderlich sind, dann wird man sich dem nicht widersetzen können.« Dem widersprach der stellvertretende Landesbeauftragte für den Datenschutz Schleswig-Holstein, Johann Bizer: Mautdaten dürfen ebenso wenig wie die Telekommunikationsdaten das Fahndungsreservoir der Inneren Sicherheit werden. Zu befürchten ist, dass die beabsichtigte Durchbrechung der Zweckbindung erst der Beginn ihrer völligen Auflösung sein wird.« Anlässlich einer Umfrage befürworteten 77% der Befragten einen Einsatz der LKW-Maut-Daten »bei der Verbrecher- und Terroristenfahndung«. Gegen diesen Vorstoß von Schäuble sprachen sich 18% aus. Unentschieden waren 5% (Borchers www.heise.de 26.11.2005; Bauchmüller/Prantl SZ 28.11.2006, 1, 4; PE ULD SH 28.11.2005; SZ 02.12.2005, 5; Eckernförder Zeitung 08.12.2006, P2).

Mehrere Länder

Sparkassen testen elektronische Signatur

Die Sparkassen Ludwigsburg, München, Nienburg, Osnabrück, Quedlinburg und Schaumburg bieten als Teilnehmer des Pilotprojektes »elektronische Signatur« als erste Banken Deutschlands die »virtuelle Unterschrift« an, ein Zertifikat und eine Chipkarte, mit denen – einer handschriftlichen Unterschrift gleichgestellt – rechtsverbindliche Aufträge über das Internet erteilt werden können.

Seit Oktober 2005 können 100 TestkundInnen wichtige Dokumente elektronisch signieren und vertrauliche Informationen in Emails verschlüsseln. Auch die Steuererklärung kann so über das Internet abgewickelt werden. Von Anfang 2006 an soll dann der Service der elektronischen Signatur sämtlichen KundInnen zur Verfügung gestellt werden. Auch Nicht-KundInnen der Sparkassen sowie Unternehmen können dieses Angebot nutzen. Neben der Chipkarte wird für den Einsatz der elektronischen Signatur ein PC mit Chipkartenleser benötigt (SZ 03./04.12.2005, 35).

Baden-Württemberg

Gesinnungstest bei Einbürgerung von Muslimen

Muslime in Baden-Württemberg, die deutsche Staatsbürger werden sollen, werden vom 01.01.2006 an Hand eines 30-Fragen-Katalogs überprüft. Der Innenminister des Landes, Heribert Recht (CDU) äußerte Zweifel, dass man bei Muslimen generell davon ausgehen könne, dass ihr Bekenntnis zur demokratischen Grundordnung bei der Einbürgerung auch ihrer wahren inneren Einstellung entspreche. Um die Gesinnung der Noch-Ausländer zu überprüfen, wird in einer Verwaltungsvorschrift ein Test mit 30 Fragen empfohlen. Gefragt wird u.a. nach der Einstellung zu Blutrache und Zwangsheirat, zur Gleichberechtigung von Mann und Frau sowie zu Gewalt in der Ehe: »Hätten Sie bei bestimmten Berufen Schwierigkeiten, eine Frau als Autoritätsperson anzuerkennen?« Auch ist die Frage vorgesehen, wie man sich verhalten würde, wenn bekannt würde, dass der eigene volljährige Sohn homosexuell ist und mit einem Mann zusammenleben möchte.

Eine Kabinettsbefassung erfolgte nicht. Als die Sache öffentlich wurde, regte sich auch Protest beim kleineren Regierungspartner FDP. Der Justizminister Ulrich Goll, zugleich Ausländerbeauftragter der Landesregierung, reklamierte ein Mitspracherecht und wollte sich für eine Überarbeitung des Bogens und für eine Ausweitung auf alle Antragsteller für Einbürgerungen einsetzen: »Wenn man auf einzelne Gruppen zielt, trägt das nur weiter zur Abschottung bei.« Manche Passagen des Fragebogens wären zu »naiv«. Deutlicher wurde die bayerische FDP-Landesvorsitzende Sabine Leutheusser-Schnarrenberger. Sie forderte, den umstrittenen »Gesinnungstest« für muslimische Einbürgerungsanwärter »umgehend wieder zurückzuziehen«. Die Fragen seien »juristisch sehr bedenklich«, zeugten von inakzeptabler »Gesinnungsschnüffelei« und bewirkten »Diskriminierung« und »Stigmatisierung«. Der »Gesprächsleitfaden« sei »mit der Politik der FDP für Integration nicht vereinbar«. Ministerpräsident Günther Oettinger (CDU) stärkte dagegen seinem Innenminister den Rücken. Er halte eine »eingehende Überprüfung des Bekenntnisses« bei allen Einbürgerungsverfahren »für selbstverständlich notwendig«.

Die Opposition aus SPD und Grünen möchte den Gesinnungstest wieder ganz abschaffen. Die SPD-Landeschefin Ute Vogt meinte: »Alle Bemühungen um Integration ausländischer Mitbürger werden da zunichte gemacht«. Die stellvertretende Fraktionsvorsitzende der Grünen Brigitte Lösch sprach von einem »unglaublichen Vorgang der Diskriminierung«.

Nachdem die öffentliche Kritik an dem Rech-Erlass bundesweit diskutiert wurde, äußerten sich auch aus der CDU kritische Stimmen zum Fragebogen. Die stellvertretende Vorsitzender der CDU-Bundestagsfraktion Katharina Reiche meinte, die Fragen seien »überzogen«. Das Deutsch-Türkische Forum (DTF) in der CDU kündigte eine Kampagne zum Stopp des Fragebogens an. Der DTF-Vorsitzende Bülent Arslan erklärte, der Einbürgerungstest sei integrationsfeindlich, ausgrenzend und verfassungsrechtlich bedenklich. Auch die meisten unionsgeführten Länder wollen derlei Befragungen nicht übernehmen. Lediglich Hessen erklärte, dem Beispiel folgen zu wollen. Niedersachsen erwägt, stattdessen einen Grundgesetzkurs für Einbürgerungswillige einzuführen. Bundesinnenminister Wolfgang Schäuble verteidigte die Praxis von Baden-Württemberg. Dass sich die Landesregierung Gedanken über die Einbürgerung mache, sei doch »wahrlich den Schweiß der Edlen wert. Die Frage, wie Männer und Frauen in Deutschland zusammenleben wollen, muss verbindlich beantwortet werden.« Am 19.01.2006 diskutierte der Bundestag auf Antrag der Grünen den Einbürgerungstest, der von allen Fraktionen außer der CDU/CSU abgelehnt wurde. Deren Sprecher Clemens Binninger meinte, mit dem Gesprächsleitfaden setze die Stuttgarter Landesregierung nur die Beschlüsse der rot-grünen Koalition zum Staatsangehörigkeitsrecht um.

Die muslimischen Verbände lehnen den Leitfaden einhellig ab; der Zentralrat der Muslime (ZMD) erwägt eine Verfassungsklage. Der Vorsitzende des Islamrates, Ali Kizilkaya, meint: »Die hier lebenden Muslime, die sich um Integration und daraus folgend auch um Einbürgerung bemühen, können dies nur als Schlag ins Gesicht empfinden.« Es sei ein Verstoß gegen den Gleichheitsgrundsatz des Grundgesetzes, wenn solche Fragen ausdrücklich nur Muslimen gestellt würden. Scharfe Kri-

tik kam aber auch vom Zentralrat der Juden, deren Präsident Paul Spiegel meinte, es handele sich bei der Befragung um einen »unbedachten Schnellschuss, der schleunigst ernsthaft überprüft werden muss«. Der Vorsitzende der katholischen Deutschen Bischofskonferenz, Kardinal Karl Lehmann, kritisierte die »staatliche Gewissensprüfung«. Die meisten Menschen verspürten eine grundsätzlich Abneigung, von den Behörden über ihr Denken ausgefragt zu werden. Der Ratsvorsitzende der Evangelischen Kirche in Deutschland (EKD) Wolfgang Huber hatte sich nach einer entsprechende Bitte um Kritik durch den ZMD für »nicht zuständig« erklärt; Baden-Württembergs Landesbischof hatte Verständnis für den Test geäußert.

Nach anhaltender bundesweiter Kritik an dem Einbürgerungstest schwächte das Innenministerium Baden-Württemberg die Befragungspraxis ein wenig ab. In einer Verwaltungsvorschrift des Ministeriums werden die Behörden nun darauf hingewiesen, dass der Gesinnungstest nicht generell auf Muslime angewendet werden solle, sondern nur, wenn Zweifel an der Verfassungstreue des Bewerbers bestünden. Die tatsächlich gestellten Fragen sollten dem »Sprach- und Bildungsniveau« der Antragsteller angepasst werden. Der Fragenkatalog sei nur »ein Hilfsmittel«. Die Verordnung sei, so das Ministerium, keine Entschärfung, sondern lediglich eine Klarstellung. Der Sachgebietsleiter der Stuttgarter Einbürgerungsbehörde meinte dagegen, dass der Rundbrief zur Folge habe, »dass nicht mehr so viele Ausländer befragt werden müssen«. In Baden-Württemberg sind 60% aller Einbürgerungswilligen Muslime. Die SPD-Oberbürgermeisterin von Heidelberg Beate Weber hatte angekündigt, dass ihre kommunalen Behörden den Leitfaden des Innenministeriums nicht anwenden würden.

Kommentar der Süddeutschen Zeitung: »Was halten Sie davon, dass in Deutschland Homosexuelle öffentliche Ämter bekleiden?« Ein strenger Katholik käme da ins Grübeln. Hat nicht der jetzige Papst Benedikt XVI. alle Katholiken aufgefordert, sich der öffentlichen Aufwertung gelebter Homosexualität zu widersetzen? ... Ein Islamist, der eine Parallelgesellschaft mit Ehrenmord und Tschador wünscht, kann unverdächtige Antworten geben: Die Tarquia, die Verstellung um des Glaubens willen, ist aus seiner Sicht geboten, wenn der schwäbische Beamte mit dem Fragebogen winkt« (KN 31.12.2005, 2; Gaserow FR 07.01.2006, 1, 4; SZ 06.01.2006, 6; SZ 07./08.01.2006, 4, 8; SZ 09.01.2006; SZ 10.01.2001, 6; Preuß SZ 13.01.2006, 6; Dörries/Esslinger/Preuß SZ 17.01.2006, 8; Schiegl SZ 20.01.2006, 5; SZ 21./22.01.2006, 6; SZ 23.01.2006, 6; SZ 01.02.2006, 5; Bartsch/Schmidt/Wassermann Der Spiegel 2/2006, 44 f.; zu Einbürgerungen in Großbritannien und Österreich s.u. S. 33 u. 35).

Bayern

Versteckte Kamera in Münchner Bordell

Als die Münchner Polizei ein neu eröffnetes Bordell am Stahlgruberring wegen Drogen- und Menschenhandel mit einer Großrazzia überzog, stellten sie nicht nur vier Gramm Kokain, sondern auch eine Videokamera sicher. In einem Zimmer im ersten Stock war die versteckte Kamera mit zwei Mikrofonen installiert. In der Zeit von der Eröffnung am 15.02. bis zur Entdeckung am 02.03.2006 wurden damit offensichtlich Aufzeichnungen angefertigt. Ob die Videos als Pornos verwendet oder Gäste damit erpresst werden sollten, ist noch unklar. Die Polizei rief die Kunden, die dort »sexuelle Leistungen erhielten«, auf, sich mit dem zuständigen Dezernat in Verbindung zu setzen. Vertraulichkeit werde garantiert. Ermittelt wird jetzt nicht nur wegen Zuhälterei u.a., sondern auch wegen der Verletzung persönlicher Lebensbereiche (SZ 15.03.2006, 33).

Bayern

PAG mit vielen informationellen Befugnissen

Die CSU-Mehrheit im bayerischen Landtag beschloss am 14.12.2005 eine Novellierung des Polizeiaufgabengesetzes (PAG), mit dem die Staatsregierung die Polizei im Kampf gegen Terror und organisierte Kriminalität schlagkräftiger machen möchte. In Bayern darf die Polizei künftig Telefone und Handys anzapfen, wenn sie meint, damit schwere Straftaten verhindern und Gefahren abwehren zu können. Geschützte Berufsgruppen wie Anwälte, Priester, Abgeordnete und Ärzte sollen nicht belauscht werden. Die Polizei soll das Abhören einstellen, wenn die Abgehörten mit Familienmitgliedern über Privates sprechen. Nach Ende der Überwachung sollen die Betroffenen von der Polizei über die Maßnahme informiert werden. Bisher waren Abhörmaßnahmen nur erlaubt, wenn die Ermittler davon ausgingen, dass eine Straftat bereits begangen worden ist. Telefonate dürfen nun auch unterbrochen oder verhindert werden. Geregelt ist weiter das präventive Abhören von Wohnungen. Erlaubt wurde zudem die automatisierte Überwachung von Autokennzeichen (Kfz-Kennzeichen-Scanning). Neu ist schließlich nach dem Gesetz der Einsatz – im Rahmen eines kontrollierten Modellprojektes – von Elektroimpulsgeräten, sog. »Tasern«.

Der PAG-Novelle war eine mehr als zweijährige Debatte über das präventive Abhören vorangegangen. Ein erster Entwurf wurde von der CSU bereits 2003 vorgelegt, nach heftigen Protesten aber wieder zurückgenommen (DANA 2/2003, 16 f.). Der Vorsitzende des Innenausschusses im Landtag, Jakob Kreidl (CSU), meinte, das nun verabschiedete Gesetz sei verfassungskonform: »Wir haben eine Lösung gefunden, die verantwortbar ist«. Der Rechtsstaat müsse »alle Möglichkeiten« nutzen, um Terroranschläge zu verhindern. Das neue PAG gewährleiste »die Vorreiterrolle Bayerns bei der inneren Sicherheit«. Innenminister Beckstein lobte das Gesetz ebenso: »Terroristen, Kinderpornohändler, grenzüberschreitend tätige organisierte Banden und Menschenhändler planen ihre Taten via Telefon und in konspirativen Wohnungen. Um diesen Bedrohungen effektiv begegnen zu können, müssen wir mit modernsten technischen Möglichkeiten dort ansetzen, wo diese Straftaten geplant werden, um die Tatausführung – wann immer möglich – zu verhindern. Die Bayerische Polizei wird von den neuen Befugnissen deshalb konsequent, aber mit dem gebotenen Augenmaß Gebrauch machen.«

SPD und Grüne warnten bei der Verabschiedung des Gesetzes vor einer Aushöhlung der Bürgerrechte; die CSU schieße über das Ziel hinaus. Die rechtspolitische Sprecherin der Grünen, Christine Stahl, kritisierte: »Wir haben die Pflicht darauf zu achten, dass die Demokratie nicht scheibchenweise stirbt.« Zwar könne man der Polizei durchaus präventive Maßnahmen an die Hand geben. Das neue PAG gehe aber zu weit und sei ein unverhältnis-

mäßiger Eingriff in die Grundrechte. Der SPD-Rechtsexperte Franz Schindler ergänzte: »Es gibt keinen Lebensbereich, in dem es noch eine Garantie gibt, nicht Objekt der Beobachtung zu werden – wenn auch zufällig und gut gemeint.« Notwendig seien nicht mehr Befugnisse für die Polizei, sondern eine Modernisierung der veralteten Ausrüstung. Die SPD enthielt sich großteils bei der Abstimmung, teils stimmte sie dagegen. In ihrer Fraktion war das PAG vor allem zwischen Rechts- und Innenpolitikern umstritten. Die Grünen lehnten das Gesetz durchgängig ab. Regierung wie Opposition rechnen damit, dass gegen das Gesetz, das bei einer Anhörung im Frühjahr 2005 auf große Skepsis bei den Experten stieß, Verfassungsbeschwerden eingelegt werden (Stroh SZ 15.12.2005, 34; www.heise.de 14.12.2005; PM 511/05 v. 14.12.2005 d. StMI Bayern; vgl. DANA 2/2004, 26; 3/2004, 29; 1/2005, 21; 2/2005, 36).

Brandenburg

Kabinett will dauerhafte Videoüberwachung

Ein Bericht des brandenburgischen Innenministeriums über die fünfjährige Erprobung der Videoüberwachung öffentlicher Plätze an vier Standorten kommt zu dem Ergebnis, dass sich diese umstrittene Methode bewährt habe. In dem am 13.12.2005 vom Kabinett beschlossenen Bericht wird festgestellt, dass an allen Standorten die Diebstahlskriminalität gesunken sei, weshalb nun die Videoüberwachung im Polizeigesetz dauerhaft verankert werden soll.

Die Versuchsinstallation war an den Bahnhofsvorplätzen Potsdam, Erkner und Bernau sowie im Außenbereich einer großen Discothek in Rathenow vorgenommen worden. Das Projekt wurde von der Universität Greifswald/Mecklenburg-Vorpommern mit einem kriminologisch-soziologischen und einem juristischen Gutachten wissenschaftlich begleitet. Danach sank die Kriminalität im Bereich der Bahnhofsvorplätze Potsdam und Erkner sowie vor der Discothek um 30 bis 60%. Eine befürchtete Verdrängung der Straftaten in angrenzende Gebiete sei nicht eingetreten. Vielmehr sei auch dort die Kriminalität deutlich zurückgegangen. In Bernau seien die Ergebnisse dagegen sehr schwankend gewesen. Die jährlichen Kosten betrugen rund 255.000 Euro. Der Aufbau kostete einmalig knapp 60.000 Euro.

Von der CDU-Fraktion im Landtag wurde umgehend ein Gesetzentwurf vorgelegt, der die Videoüberwachung generell für viele Standorte verankert und die permanente nicht nur anlassbezogene Aufzeichnung erlaubt. Über Standorte sollen danach die Polizei und auch die Kommunen eigenständig entscheiden können. Gemäß dem CDU-Innenexperten Sven Petke kämen vor allem größere Städte in Betracht: »Ich will ja nicht die märkischen Kiefern beim Wachsen filmen.« Unabhängig von Kriminalitätsschwerpunkten sollte die Überwachung an allen Orten möglich sein, an denen sich viele Menschen begegnen. Die Aufzeichnungen müssten mindestens eine Woche gespeichert werden können, da manche Straftat erst nach Verzögerung entdeckt werde.

Die Polizeigesetznovelle ist für das erste Halbjahr 2006 vorgesehen. Insofern bestünde Einvernehmen mit dem Koalitionspartner SPD. Deren Sprecherin Britta Stark favorisiert statt fester Kameras den mobilen Einsatz, um auf Entwicklungen flexibel reagieren zu können. Über die Standorte könne der Innenausschuss entscheiden. Aufzeichnungen sollten rund um die Uhr laufen, aber spätestens nach 24 Stunden gelöscht werden: »Das Recht auf informationelle Selbstbestimmung ist ein hohes Gut.« Die erfolgreiche Polizeiarbeit mit Hilfe von Aufzeichnungen nach den Attentaten in London hätten gezeigt, dass diese Einrichtungen »sehr hilfreich sein können« (Benirschke, www.heise.de 13.12.2005; www.heise.de 22.01.2006).

Bremen

Datei für Stalker

Seit September 2005 erfasst das Bremer Landeskriminalamt (LKA) Stalker, die ihren Opfern nachstellen und sie mit Psychoterror drangsalieren, in einer Gefährder-Datei. Bremen ist damit – nach eigenen Angaben – das erste Bundesland, das Stalker und Täter von häuslicher Gewalt, also z.B. prügelnde Ehemänner, derart speichert. Die Beamten können im Computer auch erkennen, ob es richterliche Anordnungen gegen die Täter gibt. Innensenator Thomas Röwekamp (CDU): »Wir können dieses System anderen Bundesländern empfehlen. Es hilft den Polizisten, die Lage vor Ort einzuschätzen und besser eingreifen zu können.« Bislang sind in der Datei 55 Gefährder registriert, darunter 49 Stalker und mehr als 450 Fälle. Bremen nimmt eine Vorreiterrolle bei der Stalking-Bekämpfung ein. Die Datei wurde eingerichtet, nachdem ein Mann seine Ehefrau an ihrer Arbeitsstelle im Bremer Maritim-Hotel ermordet hatte. Ein von Berlin eingebrachter Gesetzentwurf, der Stalking zur Straftat macht, wird von vielen Landesregierungen unterstützt (Der Spiegel 47/2005, 20).

Hessen

Massengentest soll Kindervergewaltiger ermitteln

Auf der Suche nach dem Vergewaltiger eines fünfjährigen Mädchens hat die Polizei im südhessischen Viernheim Anfang Dezember 2005 4.600 Männer aufgefordert, sich an einem Massengentest zu beteiligen. Die Fünfjährige war Anfang Oktober 2005 im Bereich eines Spielplatzes auf einem Kirchengelände der Stadt im Landkreis Bergstraße vergewaltigt worden (SZ 10./11.12.2005, 12).

Niedersachsen

Polizei kontrolliert Journalisten-Telefone

Auf Antrag der Staatsanwaltschaft Braunschweig und nach richterlichem Beschluss wurden von der Polizei nach mehreren Tagen in den Jahren 2003 und 2004 die Verbindungsdaten der Handy- und Festnetz-Telefonanschlüsse der Wolfsburger Allgemeinen Zeitung (WAZ) sowie der Privatanschlüsse von zwei Journalisten abgefragt und gespeichert worden. Auf eine parlamentarische Anfrage hin teilte das Justizministerium mit, es sei lediglich ermittelt worden, wann und wo telefoniert worden ist. Die Ermittlungen richteten sich in erster Linie gegen zwei Polizeibeamte wegen des Anfangsverdachtes des Verrats von Dienstgeheimnissen, außerdem gegen eine Journalistin wegen des Verdachtes der Anstiftung. Die Reporter hatten in zwei Fällen über zwei Kriminalfälle berichtet: den Fund eines to-

ten Babys und den Überfall auf ein Geschäft in der Wolfsburger Innenstadt. Die Vorwürfe gegen die Beschuldigten erwiesen sich als haltlos. Laut Angaben handelte es sich um zwei Berichte, die der Polizei »nicht genehm gewesen« seien. Es habe sich, so die Landesregierung, um Informationen gehandelt, die nur polizeiintern bekannt gewesen sind. Die hannoversche Verlagsgesellschaft Madsack, die die WAZ herausgibt, der Deutsche Journalisten-Verband (DJV), die Deutsche Journalistenunion (dju) sowie die Oppositionsparteien SPD und Grüne verlangten eine lückenlose Aufklärung in dieser »Schnüffelaffäre« (DJV). Der innenpolitische Sperecher der Grünen, Hans-Albert Lennartz sprach von einem »Anschlag auf die Pressefreiheit« (Langrock-Kögel SZ 02.03.2006, 7, 17; Welt kompakt 28.02.2006, 5).

Nordrhein-Westfalen

Neues Polizei-Auskunftssystem Polas

»Polas« ist das Polizeiliche Auskunftssystem der Landespolizei von Nordrhein-Westfalen. Über einen Zentralrechner in Duisburg verbindet das System 26.000 Polizeirechner in über 450 Dienststellen. Innerhalb weniger Sekunden ist der Zugriff auf über 7,5 Mio. Datensätze möglich. Polas ist auch das Zugangssystem für das bundesweite INPOL-System sowie auf internationale Polizei-Datenbanken. Gegenüber dem Vorgängersystem Pikas, das nur von geschulten Kräften zu bedienen war, hat Polas den Vorteil leicht verständlicher Benutzeroberflächen, die für alle Polizistinnen und Polizisten leicht handhabbar sind (SZ 20.01.2006, 2).

Ausländische Datenschutznachrichten

Großbritannien

Neuer Einwanderungstest prüft »Britishness«

Die Londoner Regierung hat einen Fragebogen mit 200 Fragen vorgelegt, von dem 24 jeweils ausgewählte Fragen ab sofort alle ausfüllen müssen, die britische Staatsbürger werden wollen. Mit dem »Britishness Test« soll sichergestellt werden, so Staatsminister für Einwanderung und Staatsbürgerschaft Tony McNully, dass Neubürger »ihre Rechte und Pflichten verstehen« und generell bereit sind, Untertanen ihrer Majestät zu werden. Für die 24 Fragen haben die Staatsbürgerschaftsbewerber großzügige 1 ½ Stunden Zeit. Bestanden hat, wer mindestens 18 richtige Antworten gibt. Im Gegensatz zu anderen Ländern mit ähnlichen Tests kann man in Großbritannien die Prüfung beliebig oft in einem der insgesamt 90 über das Land verstreuten Testzentren wiederholen. Im Schnitt beantragen 100.000 Männer und Frauen jedes Jahr den britischen Pass. Im Jahr 2004 wurden sogar 140.000 Anträge genehmigt. Gefragt wird nach gemeinschaftskundlichen Themen zum Land, zur EU und zum Commonwealth. Einwanderungsverbände haben den Fragebogen als zu schwierig gerügt. Sie wiesen darauf hin, dass sogar im Vereinigten Königreich geborene und aufgewachsene Lehrer bei einem Probelauf mit Pauken und Trompeten durch die Prüfung gefallen sind. Dem erwiderte Minister Mc Nully, er selbst habe bis auf eine alle Fragen richtig beantworten können. Es sei wie bei der Führerscheinprüfung: »Wer die Fahrlizenz seit Jahren besitzt, würde sie heute nicht mehr bestehen. Anfänger hingegen haben alle Antworten vor der Prüfung gebüffelt« (Koydl SZ 02.11.2005, 8).

Großbritannien

Schadenersatz wegen Spam

Zum ersten Mal gelang es einem britischen Internet-Nutzer, eine Entschädigung von einem Unternehmen zu erstreiten, das ihm unerwünschte Werbe-Emails, sog. Spam, geschickt hatte. Nigel Roberts, Internet-Experte und Jurist, verklagte die Fa. Media Logistics UK Ltd. auf der Grundlage der Anti-Spam-Richtlinie der Europäischen Union. Das Unternehmen hatte ihn mit Spam belästigt. Roberts gewann den Prozess und einigte sich in einem Vergleich auf einen Schadenersatz in Höhe von 300 britischen Pfund, ca. 437 Euro. Deutschen Spam-Opfern nutzt Roberts Erfolgt wenig, da die Europäische Anti-Spam-Richtlinie nur einen Rechtsrahmen vorgibt, der national mit konkreten Klage- und Strafmöglichkeiten umgesetzt werden muss. Der Gesetzgeber gewährt in Deutschland Privatpersonen nicht die Möglichkeit, Geld von Spam-Firmen zu erstreiten. Dies steht hier nur Institutionen zu (Der Spiegel 2/2006, 58).

Großbritannien

Kinder dürfen für Passfotos lächeln

In Großbritannien sind die Regeln für Passfotos von Kindern wieder gelockert worden. Viele Eltern waren gescheitert, ihr Kind für das Passfoto zu einem »neutralen« Gesichtsausdruck mit dem Blick geradeaus und einem geschlossenen Mund zu bringen. Im Jahr 2005 wurden in weniger als drei Monaten mehr als 15.000 Kinderausweisanträge abgelehnt, weil die Fotos nicht den Vorgaben entsprachen, zu denen etwa auch ein matter Teint gehört. Jetzt dürfen Kinder auf den Bildern sogar wieder lachen (SZ 13.01.2006, 10; vgl. DANA 4/2005, 20 f., 29).

Großbritannien

Staatliche Videoüberwachung für Jedermann

Einwohner des Londoner Stadtteils Shoreditch werden sich künftig gegenseitig überwachen können. Im März 2006 wird ein von der Regierung finanziertes Pilotprojekt die rund 400 öffentlichen Überwachungskameras des Viertels mit den Computern von zunächst 1.000 privaten Haushalten verbinden. Über ein Breitbandkabel und einen neu geschaffenen Fernsehkanal werden Livebilder der Kameras in die einzelnen Wohnungen gesendet und sind dort wahlweise auf dem Fernseher oder einem Computermonitor zu sehen. Hin-

weise auf Randalierer oder mutmaßliche Kriminelle können dann online und anonym an die Polizei übermittelt werden. Außerdem bietet das System die Möglichkeit, verdächtige Personen mit einer Online-Galerie bekannter Krimineller zu vergleichen. Befürworter erhoffen sich Hilfe bei der Bekämpfung der Kriminalität in Shoreditch. Das Viertel gehört zu den ärmsten Stadtteilen in Großbritannien. Sollte die Testphase erfolgreich sein, so soll der »Service« allen 20.000 Haushalten angeboten werden. Bürgerrechtler lehnen das Projekt ab (Der Spiegel 3/2006, 83).

Frankreich

Anti-Terror-Gesetz verabschiedet

Nach der Nationalversammlung hat auch der französische Senat das von Innenminister Nicolas Sarkozy eingebrachte Anti-Terror-Gesetz verabschiedet: »Was in New York, Madrid und London geschehen ist, das kann morgen auch in Frankreich passieren.« Damit hat Frankreich nach Großbritannien die schärfsten Bestimmungen in Europa. So kann die Polizei Verdächtige nun vier statt bisher drei Tage zum Verhör festhalten, ohne dass sie dem Haftrichter vorgeführt werden müssen. Im grenzüberschreitenden Verkehr soll die Personenkontrolle wieder verschärft werden. Eine intensivere Videoüberwachung wird ermöglicht. Allein in Paris wird die Zahl der Überwachungskameras auf 23.000 geschätzt. Künftig sollen noch mehr Metro-Bahnsteige, öffentliche Gebäude und exponierte Plätze überwacht werden.

Das Gesetz gestattet vor allem eine intensivere Sammlung von Informationen. Generell wird die Überwachung des Internets und das Abhören von Telefonaten erleichtert. Betreiber von Servern und von Internet-Cafés, die jedem anonymen Benutzer zur Verfügung stehen, werden verpflichtet, alle Verbindungsdaten ein Jahr lang aufzubewahren. Diese Passage wurde von der nationalen Datenschutzbehörde CNIL (Commission nationale informatique et libertés) kritisiert. Der Verfassungsrat (Conseil d´Etat), das oberste französische Verwaltungsgericht, das im Vorfeld der Gesetzesverabschiedung zu Rate gezogen werden kann, hatte dieser Regelung Unbedenklichkeit bescheinigt. Während die Regierungspartei geschlossen für das Gesetz stimmte, waren die Sozialisten gespalten. Grüne und Kommunisten votierten sowohl in der Nationalversammlung als auch im Senat gegen das neue Gesetz, das sie als »freiheitstötend« bezeichneten. Die sozialistische Senats-Fraktion will den Verfassungsrat gegen das gesamte Gesetz anrufen. Der Widerstand gegen das Gesetz kam bisher aber vorwiegend von außerparlamentarischen Vereinigungen, z.B. von Anwaltsvereinigungen und Bürgerrechtsorganisationen wie der traditionsreichen Liga für Menschenrechte. »Wir wollen keine Verhältnisse wie in London, wo man 300 Mal am Tag gefilmt wird«, meinte ein Sprecher der Gruppe »Lächeln Sie, Sie sind im Bilde« (Kröncke SZ 25.11.2005, 8; SZ 23.12.2005, 1; Schmid Telepolis 30.11.2005).

Frankreich

Motorrad-Polizisten mit versteckter Kamera

Zivile Polizei-Motorradstreifen machen mit versteckter Kamera im Helm künftig Jagd auf Verkehrssünder. Die verdeckten Fahnder sollen vor allem Motorradrasern nachstellen. Auch verfolgen sie Autofahrer, die z.B. unerlaubt am Steuer telefonieren. Die Filme werden ausgewertet, die Verkehrssünder anschließende zur Kasse gebeten. Die Originalfilme sollen auch im Verkehrsunterricht an Schulen eingesetzt werden (SZ 05./06.01.2006).

Frankreich

Metalldetektoren und Kameras an Schulen

Um die Gewalt gegen Lehrer einzudämmen, will der französische Erziehungsminister Gilles de Robien drakonische Maßnahmen umsetzen. Am 16.12.2005 war eine französische Lehrerin in dem Pariser Vorort Etampes mitten im Unterricht von einem Schüler mit einem Messer attackiert worden. Der Minister meint nun: »Sozialstationen haben sich bereits an den Unterrichtsanstalten bewährt, warum sollte es nicht eine ständige Polizeibereitschaft in einem kleinen Raum neben dem Büro des Rektors geben?« Die Gegenwart von Polizisten in bestimmten Schulen solle »alltäglich gemacht« werden, um einen »einfachen, natürlichen Dialog mit der Lehrerschaft« zu etablieren und damit Übergriffen vorzubeugen. Als weitere Maßnahme will Robien Überwachungskameras und Metalldetektoren an Schulen installieren, um das Tragen von Waffen zu unterbinden. »Selbst wenn es jedes Mal, sobald man die Initiative in diesem Bereich ergreift, eine Lawine von Kritik gibt«, werde er unbeirrt bleiben. Sein Vorgänger Francois Fillon hatte noch auf Vorschläge des Innenministers Nicolas Sarkozy, Verbindungspolizisten in den Schulen zu etablieren, gemeint: »Polizei hat in der Schule nichts zu suchen« (Kröncke, SZ 21.12.2005, 6).

Frankreich

Elektronische Fessel für Serientäter

Gefährliche Serientäter können künftig in Frankreich nach Verbüßen ihrer Haftstrafe mit einem elektronischen Armband versehen werden, mit dem automatisch deren Aufenthaltsort festgestellt werden kann. Gegen die Stimmen der linken Parteien stimmte das Parlament dieser »Sicherheitsmaßnahme« für Gewalt- und Sexualtäter zu. Sie darf maximal sechs Jahre lang bei einem Täter angewandt werden, der zumindest zu sieben Jahren Haft verurteilt worden ist. Der Täter muss zudem dem Tragen des Armbandes zustimmen (SZ 26./27.11.2005, 7).

Niederlande

Oppositionsüberwachung durch Nachrichtendienst AIVD

Der niederländische Nachrichtendienst AIVD ist in großer Verlegenheit: Ein Mitarbeiter hat zwei Disketten mit vertraulichen Informationen in einem Mietauto liegen lassen. Die als Staatsgeheimnis gehandelten Daten aus den Jahren 1995 bis 2002 wurden dem Fernsehjournalisten Peter de Vries übergeben, der eine populäre Sendung verantwortet. Nach Angaben von de Vries enthalten die Disketten Berichte darüber, wie der Geheimdienst Umweltverbände, die molukkische Exilbewegung oder Linksextremisten infiltrierte, was er über Lokalpolitiker oder prominente Sozialdemokraten weiß und welche

Hinweise er als »schmutzige Wäsche« innerhalb der liberalen Regierungspartei D66 hat. Besonders brisant seien die »sehr kompromittierenden« Informationen über »sexuelle Eskapaden« mit minderjährigen marokkanischen Jungen des im Mai 2002 ermordeten Politikers und bekennenden Homosexuellen Pim Fortuyn. Der niederländische Geheimdienst hat den Journalisten aufgefordert, die Diskette unverzüglich zurückzugeben. Peter de Vries, der mit einer neuen Partei an den Parlamentswahlen 2007 als Spitzenkandidat teilnehmen will, erklärte, er werde keine Namen und Kontaktadressen von AIVD-Agenten oder befreundeten Diensten nennen. Über die Ausspähung von Fortuyn und die Arbeitsweise der niederländischen Agenten müsse er aber wohl berichten.

Der Skandal ist einer von mehreren Fehlschlägen des AIVD in der letzten Zeit. So hatte ein Dolmetscher geheime Informationen an Mitglieder der militant-islamistischen Hofstadt-Gruppe weitergegeben, der auch der Mörder von Theo van Gogh angehört. Zwei Monate zuvor hatte ein AIVD-Mitarbeiter seinen Laptop mit vertraulichen Informationen im Zug vergessen. Der Rechner ist seitdem verschwunden. Eine Woche zuvor wurde durch Zufall die Identität eines AIVD-Informanten gelüftet (Weidemann, SZ 12.12.2005, 7).

Österreich

Hohe Hürden hindern Einbürgerung

Österreichs Koalition ist stolz auf das seit dem 01.01.2006 gültige weit und breit strengste bzw. abweisendste Einbürgerungsrecht. Die Fristen, wie lange ein Ausländer in Österreich zu leben hat, oder wie lange er mit einer ÖsterreicherIn verheiratet sein muss, um eingebürgert zu werden, wurden verlängert. Die Gebühren wurden so stark erhöht – auf i.d.R. 900 Euro für Erwachsene und 200 Euro bei Kindern – dass karitative Verbände dagegen protestierten. Das Anfang Dezember 2005 verabschiedete Staatsbürgerschaftsgesetz soll Einbürgerungen erschweren, Scheinehen verhindern und gute Sprachkenntnisse der NeubürgerInnen und damit eine günstige Integrationsprognose sicherstellen. Für Prominente wie Sportler und Künstler sind weiter rasche, leicht erschwerte Sonderverfahren möglich. Die Deutschprüfung hat künftig zentrale Bedeutung. Verhindert wurde, dass einzubürgernden Kindern bessere Deutschkenntnisse abverlangt worden wären als gleichaltrigen Einheimischen. Befragungen wie in Baden-Württemberg (s.o. S. 30) finden nicht statt. Dafür ist aber der Ermessensspielraum der Behörden groß und wird je nach Bundesland unterschiedlich ausgeschöpft. Zuletzt wurden auch entscheidungsreife Anträge im Vorgriff auf das verschärfte Gesetz liegen gelassen. Die Einbürgerungen gehen seit Jahren stark zurück. 2004 bekamen 41.645 AusländerInnen einen österreichischen Pass, fast 7% weniger als 2003. 2005 zählte man 26.556 in den ersten drei Quartalen, was auf einen noch entschiedeneren Rückgang hindeutet (Frank SZ 17.01.2006, 8).

USA

Patriot Act bleibt kurzfristig weiter bestehen

Der US-Kongress hat kurz vor Ablauf der umstrittenen Anti-Terror-Gesetze mit dem schönen Namen »Patriot Act« eine Verlängerung von nur 5 Wochen bis Anfang Februar 2006 beschlossen. Verhandlungsführer des Senats und des Repräsentantenhauses hatten sich zunächst am 08.12.2005 auf eine vierjährige Verlängerung geeinigt. Doch konnte das Tauziehen um 16 Vorschriften nicht beendet werden, bei denen es um umfassende Abhöraktionen wie das Anzapfen von Telefonleitungen und das Abfangen von Emails sowie die Auswertung von Daten von Firmen, Banken und Krankenhäuser geht (vgl. DANA 3/2005, 26). Das Repräsentantenhaus hatte zuvor eine Überprüfung nach 10 Jahren verlangt. Ohne die Verlängerung wären einige der Regelungen am 31.12.2005 ausgelaufen. Der Patriot Act war nach den Anschlägen des 11.09.2001 als zentrales Element der US-Regierung im Kampf gegen den Terrorismus verabschiedet worden. Die Gesetze schränken zahlreiche Bürgerrechte ein. Mehrere hochrangige Demokraten und Republikaner äußerten ihren Widerstand gegen den Kompromiss. Darin ist u.a. vorgesehen, dass Sicherheitsbehörden 30 Tage nach einer geheimen Hausdurchsuchung die davon betroffene Person informieren müssen. Wenn Behörden Daten von Bibliotheken anfordern, muss ein ziviles Gericht bestätigen, dass dies in Verbindung mit Terror-Ermittlungen geschieht. Eine Sprecherin der Bürgerrechtsgruppe ACLU (vgl. S. 36) kritisierte, dass z.B. die Bundespolizei FBI weiterhin Zugang zu privaten Daten von unschuldigen Amerikanern erhält, ohne die Relevanz für den Kampf gegen der Terrorismus beweisen zu müssen (SZ 10./11.12.2005, 9; Kornelius u. Rubner SZ 24.12.2005, 4, 7).

USA

Auslandsgeheimdienst hat Amerikaner ausspioniert

Die National Security Agency (NSA), der amerikanische Auslandsgeheimdienst, hat seit 2002 die Telefonate und Emails mehr oder weniger verdächtiger US-BürgerInnen abgehört, um Hinweise auf eventuelle Verbindungen zu ausländischen Terroristen abzufangen. Eine entsprechende Ermächtigung hatte Präsident George W. Bush der NSA, der sonst nur Operationen im Ausland gestattet sind, seit Anfang 2002 erteilt. Dass dies schlicht per Erlass, also ohne Gesetz des Kongresses und obendrein ohne richterliche Kontrolle geschah, legten ihm sogar einige republikanische Parteifreunde als Amtsanmaßung aus. Michael Hayden von der NSA musste eingestehen, dass auch Telefonate und Emails von unverdächtigen Normalbürgern abgehört worden sind. Man arbeite eng mit den großen Telekommunikationsunternehmen zusammen, um Zugriff auf internationale Kommunikationskontakte zu erhalten. Auf diese Weise seien »riesige Mengen« an Telefonaten und Internetverbindungen analysiert worden, um Verhaltensmuster von Verdächtigen zu erhalten. Regierungsvertreter beschrieben das Programm als »groß angelegte Operation zur Datensammlung«.

Das Parlamentsinstitut Congressional Research Services kam in einer für den US-Kongress erstellten Studie zu dem Ergebnis, dass die Praxis in Widerspruch zu dem FISA-Gesetz (Foreign Intelligence Surveillance Act) aus dem Jahr 1978 steht. Darin wird explizit die nachrichtendienstliche Überwachung von US-BürgerInnen im Inland von einer richterlichen Genehmigung abhängig gemacht. Die Genehmigung nach dem Gesetz durch das geheime FISA-Gericht ist seither in 18.742 Fällen ein-

geholt worden (vgl. DANA 4/2002, 41 f.). In drei Fällen haben inzwischen Anwälte die gerichtliche Überprüfung von Urteilen oder der gesetzlichen Grundlage der Verfahren wegen der illegalen Telekommunikationsüberwachung beantragt. In allen drei Fällen besteht der Verdacht, dass Erkenntnisse auf Grund der Präsidenten-Anordnung gewonnen worden sind. Die Enthüllung erfolgte durch die New York Times. Diese bestätigte, bereits seit einem Jahr von dem Vorgehen der NSA zu wissen. Aus Rücksicht auf Befürchtungen der Regierung, laufende Ermittlungen könnten gefährdet werden, habe die Redaktion zuvor auf eine Veröffentlichung verzichtet.

Bush kritisierte die Veröffentlichung der New York Times: »Diese ungenehmigte Enthüllung schadet unserer nationalen Sicherheit und gefährdet unsere Bürger. Im Ergebnis haben unsere Feinde nun Informationen, die sie nicht haben sollten.« Er erklärte, er betrachte den seit dem 11.09.2001 bestehenden Kriegszustand auch als juristisch tragfähige Ermächtigung, um »die Sicherheit unserer Nation zu verteidigen«. Er versuchte den Vorwurf, sein Vorgehen missachte die Verfassung, ins Lächerliche zu ziehen: »Wenn ich das Gesetz brechen wollte, warum würde ich dann wohl den Kongress briefen?« In der Tat hatte die Regierung nach dem 11.09.2001 regelmäßig die Geheimdienstausschüsse von Senat und Repräsentantenhaus streng vertraulich und in sehr groben Zügen über das NSA-Vorgehen informiert. Bush schickte nach entsprechenden Enthüllungen Minister und hochrangige Geheimdienstexperten nach vorne, um der Bevölkerung Sinn, Zweck und Legalität seines »Terroristen-Überwachungsprogramms« zu erklären. In der vordersten Linie Bushs steht Keith B. Alexander, Chef der NSA. Der als Techno-Freak bezeichnete Generalleutnant soll die NSA mit seinen mehr als 30.000 MitarbeiterInnen von einer Horchtruppe aus Zeiten des kalten Krieges umrüsten zu einem High-Tech-Geheimdienst und einer Anti-Terror-Einrichtung des 21. Jahrhunderts: »Wir suchen nicht länger eine sowjetische Division. Wir müssen unter Umständen eine Einzelperson finden, die uns bedroht. Wenn wir überhaupt etwas übermäßig schützen, dann sind dies die Freiheitsrechte unserer Bürger.« Der NSA verweist zur Rechtfertigung auf wichtige Fahndungserfolge. So sei z.B. aufgedeckt worden, dass ein arabisch-stämmiger US-Bürger im Jahr 2003 geplant habe, die Brooklyn Bridge in New York zu sprengen. Der Angeklagte hatte sich später schuldig bekannt.

Im Zuge der Diskussion um die NSA-Lauschangriffe legte ein ranghoher US-Bundesrichter aus Protest sein Amt am Gericht für die Überwachung der Ausländischen Geheimdienste (FISA) nieder. Außerdem wurde bekannt, dass die Bundespolizei FBI und das Energieministerium tausende Wohnhäuser und Arbeitsplätze von Muslimen sowie Moscheen ohne richterliche Genehmigung auf radioaktive Spuren hin untersucht haben. Ziel des streng geheimen Programms sei es gewesen herauszufinden, ob z.B. in Moscheen an Bomben gebaut werde. Allein im Großraum Washington wurden demnach bis zu 120 von Muslimen besuchte Orte überwacht, weitere in New York, Chicago, Seattle, Detroit und Las Vegas. Regierungsbehörden bestätigten auch, dass Geigerzähler zum Aufspüren radioaktiver Strahlung in Häfen, U-Bahn-Stationen und öffentlichen Plätzen installiert worden sind.

Bush versucht sich für die Kongresswahlen im November 2006 als Garant der inneren Sicherheit profilieren. Auch die Demokraten rüsten sich für die politische Schlacht um Sicherheit und Freiheit. So hat nach deren Ansicht z.B. der Irak-Krieg die USA nicht sicherer gemacht. Der frühere Mehrheitsführer der Demokraten sagte, dass er das nicht gewollt habe, als der Kongress drei Tage nach dem 11.09.2001 Bush »alle nötigen Mittel« im Kampf gegen den Terror erlaubt habe. In Bezug auf die NSA-Aktivitäten meinte aber der demokratische Senator John Kerry: »Wir alle unterstützen die Überwachung.« Nur genüge dazu eben nicht ein simples Dekret (Wernicke SZ 17./18.12.2005, 9; Wernicke SZ 19.12.2005, 7; Wernicke SZ 21.12.2005, 7; SZ 27.12.2005, 10; Klüver 30.12.2005, 4, 8; Klüver SZ 03.01.2006, 4; SZ 09.01.2006, 7; Wernicke SZ 26.01.2006, 10).

USA
American Civil Liberties Union

Eine der engagierten, für Datenschutz in den USA eintretenden nichtstaatlichen Organisationen (NGO) ist die Amerikanische Bürgerrechtsunion (American Civil Liberties Union – ACLU). Der Vorgänger der ACLU ist das 1917 gegründete National Civil Liberties Bureau (NCLB). 1929 wurde es in ACLU umbenannt. Zu ihren Aufgaben gehörte es damals, AusländerInnen vor Abschiebung zu schützen und US-BürgerInnen, denen Nähe zum Kommunismus vorgeworfen wurde, vor Strafprozessen zu bewahren. Die ACLU hat in der Vergangenheit immer wieder mit Klagen Aufsehen erregt, so z.B. 1954 mit dem Fall »Brown vs. Board of Education«, einem Gerichtsverfahren, das zum Ende der Rassentrennung in öffentlichen Schulen führte. Die ACLU hat derzeit ca. 400.000 Mitglieder. Den größten Zuwachs verzeichnete die Organisation nach den Terroranschlägen am 11.09.2001, als die darauf folgenden US-Sicherheitsmaßnahmen Debatten über die Verletzung von Bürgerrechten auslösten. Die ACLU ist eine der wichtigsten innerstaatlichen Kritikerinnen des Patriot Act der Bush-Regierung (s.o.). Der Hauptsitz der ACLU liegt in New York. Sie finanziert sich durch Mitgliedsbeiträge und Spenden (SZ 09.12.2005, 2).

USA
Schärfere Paparazzi-Regelungen in Kalifornien

Seit dem 01.01.2006 gelten scharfe gesetzliche Regelungen, die Prominente vor Paparazzi schützen sollen. Werden diese handgreiflich oder verursachen diese Unfälle, so müssen sie tief in die Tasche greifen und das dreifache aller Schäden erstatten, für die sie verantwortlich sind. Zudem verlieren sie alle Einnahmen, sollten die Fotos veröffentlicht werden. Die Abgeordnete Cindy Montanez, die für die Initiative mit verantwortlich ist, meint: »Jetzt werden es sich Paparazzi zweimal überlegen, ob sie in Kalifornien einen Promi verfolgen.« Die Neuregelung beeinträchtige die Rechte der Journalisten nicht. Sie ziele nur auf jene, »die das Gesetz brechen bei dem Versuch, an ihre Bilder zu kommen.« Jim Ewert, Jurist des kalifornischen Zeitungsverlegerverbandes, fürchtet dagegen, Stars könnten das Gesetz nutzen und eine Klage anzustrengen, um Fotos und entsprechende Artikel zu unterdrücken: »Wir können das Verhalten von Paparazzi nicht entschuldigen. Aber das Gesetz ist der Versuch, mit eisernen Besen zu kehren« (SZ 04.01.2006, 10).

USA

Sexualstraftäter auf der Plakatwand

Der US-Staat Mississippi will die Namen und Gesichter verurteilter Sexualstraftäter auf Plakatwänden entlang von Straßen veröffentlichen. V.a. Bilder von Tätern, die sich an Minderjährigen vergangen haben, könnten - so Don Tyler, Leiter der staatlichen Dienstleistungsbehörde - demnächst auf bis zu 100 geplanten Plakaten zu sehen sein. Ziel sei es, die Öffentlichkeit auf Straftaten aufmerksam zu machen. Auf den Plakaten, die bis zum Sommer 2006 bereitstehen sollen, werden den Plänen zufolge Fotos und Namen von Tätern, die derzeit im Gefängnis sitzen, sowie Einzelheiten über deren Vergehen veröffentlicht. Die Leiterin der Amerikanischen Union für bürgerliche Freiheiten (ACLU, S. 36) in Mississippi, Nsombi Lambright, kritisierte das Vorhaben (SZ 21.02.2006, 11).

China

Korrupte Geschäftsleute am Pranger

China will die Namen von Geschäftsleuten publik machen, denen der Vorwurf gemacht wird, Bestechungsgelder gezahlt zu haben. Eine entsprechende »schwarze Liste« soll vom Jahr 2006 an veröffentlicht werden. Die Namen von korrupten Individuen oder Firmen sollen dann rückwirkend bei Bestechungsfällen seit dem Jahr 1997 öffentlich an den Pranger gestellt werden. Dieser neueste Schritt in Chinas andauerndem, bisher nicht sonderlich erfolgreichen Kampf gegen Wirtschaftskorruption wurde von der Regierung offensichtlich wegen seiner Öffentlichkeitswirkung verkündet. Die Meldung über die schwarzen Listen wurde am 03.11.2005 prominent auf der ersten Seite der englischsprachigen »China Daily« platziert, die überwiegend von AusländerInnen gelesen wird. Die Regierung will im Ausland den Eindruck erwecken, China gehe ernsthaft gegen Korruption vor. Ob auch die Namen ausländischer Geschäftsleute veröffentlicht werden sollen, wurde nicht erwähnt.

Zwar sind die Strafen wegen Korruption drakonisch und gehen in schweren Fällen bis zur Todesstrafe. Dennoch nimmt die Korruption, insbesondere bei lokalen Kadern der Kommunistischen Partei, weiter zu, was allein im Jahr 2004 einer der vorrangigen Gründe für die 74.000 öffentlichen Proteste und Demonstrationen war. In der Realität werden in China allerdings meist nur diejenigen bestraft, die keine Beziehungen zu hochrangigen Parteikadern haben. Auch die Familien der Partei-Elite sind, von ganz wenigen Ausnahmen abgesehen, von Strafverfolgung in Sachen Korruption ausgenommen. Die jüngste Großkampagne richtete sich gegen die Korruption in der ständig von tödlichen Unfällen geplagten chinesischen Kohleindustrie (Bork SZ 04.11.2005, 11).

China

Militär-Hacker greifen USA an

Vom chinesischen Militär beauftragte Hacker haben sich nach Angaben von Alan Paller, Leiter des US-Instituts für Computersicherheit, systematisch Zugang zu Rechnernetzwerken der US-Regierung und von Unternehmen verschafft. Die Attacken seien bis in die chinesische Provinz Guangdong zurückverfolgt worden. Die eingesetzten Techniken legten nahe, dass das Militär die Angriffe geführt habe. Die Eindringlinge seien ohne »Tippfehler und Fingerabdrücke« in die Systeme eingedrungen. Betroffen waren neben Regierungsbehörden auch Auftragnehmer des Pentagon (SZ 14.12.2005, 8).

China

Umfassende Internet-Kontrolle

Nach Erkenntnissen der Opennet-Initiative (ONI) der Universitäten Toronto, Harvard und Cambridge hat China das ausgeklügeltste und effektivste System weltweit, um das Internet nach unliebsamen Informationen zu durchforsten. In einer 2005 veröffentlichten Länderstudie China schreibt ONI: »Im Gegensatz zu Filtersystemen in vielen anderen Ländern scheint das Regime in China dynamisch zu sein. Es verändert sich entlang verschiedener Achsen.« Tests hätte ergeben, dass der Zugang zu einer großen Bandbreite von Themen, die Peking als sensibel einstuft, verhindert wird – oft zu 100% auf Seiten in chinesischer Sprache, aber auch auf englischen Seiten, die nur eine Minderheit in China lesen kann. Blockiert werden z.B. Seiten, die unabhängig über das Tiananmen-Massaker 1989, Tibet, die Meditationsbewegung Falun Gong, Taiwan, Menschenrechte oder Demokratie berichten.

Nach Einschätzungen ausländischer Beobachter kontrollieren ca. 40.000 Sicherheitsbeamte in China das Internet, das dort derzeit von ca. 130 Mio. Menschen genutzt wird. Die Internationale Gesellschaft für Menschenrechte berichtet, dass mehrere hunderttausende »subversive Internet-Seiten in China gesperrt seien. Dazu gehören nicht nur die Seiten von Menschenrechtsorganisationen, sondern auch der BBC oder sehr viele Seiten mit christlichen Inhalten. Internetnutzende müssen sich registrieren lassen. Inhalte können auch nachträglich zu Staatsgeheimnissen erklärt werden. Die Besitzer der »Netzbars« wie Internet-Cafés in China genannt werden, müssen die Personalien ihrer Besucher 60 Tage lang speichern. Bei den Internet-Anbietern sind extra Angestellte dafür eingestellt, die »da mama« genannt werden, die die Einhaltung der Regeln überwachen. Die Internet-Nutzenden werden zugleich von der Regierung aufgerufen, festgestelltes Unliebsames den Behörden zu melden. Derzeit sitzen mindestens 55 sog. Cyber-Dissidenten in China in Haft. Eines der bekanntesten Opfer der staatlichen Kontrolle ist Shi Tao (DANA 4/2005, 31).

Am 25.01.2006 kündigte nun der Betreiber der größten Internet-Suchmaschine der Welt Google mit dem Start seines chinesischen Internet-Portals www.google.cn an, die vorgegebenen Zensurbestimmungen der Regierung in Peking zu übernehmen. Damit hat sich jetzt auch Google nach dem Urteil des Asienexperten der Reporter ohne Grenzen (RSF), Vincent Brossel, »als letzte« große Suchmaschine dem Druck Pekings gebeugt. Bisher hatte Google für China lediglich seine Nachrichten-Webseite Google News zensiert, indem es alle der chinesischen Regierung unliebsamen Inhalte entfernte. Über die in den USA stationierte Suchmaschine google.com/intl./zh-CN können vorerst weiter unzensiert Inhalte in chinesischer Sprache abgerufen werden, doch ist diese Webseite, die im Jahr 2002 schon einmal komplett blockiert war, langsamer als die anderen Angebote im Inland.

Die Schlacht um die chinesischen Internet-Nutzenden wird mit großer Här-

te geführt. Auch um die Bereitstellung der Infrastruktur gibt es einen harten Wettbewerb. Die Regierung kann dabei die Konditionen diktieren. Die Firma Cisco hat z.B. – so Angaben von ONI – an China eine sehr leistungsfähige Filtertechnik geliefert. Damit können mehr als 750 000 sog. Regeln definiert werden, um Viren abzufangen, aber auch um Seiten zu sperren, die bestimmte politischen Codewörter enthalten. Die jungen chinesischen Internet-Nutzenden betrachten laut einer Studie der Chinesischen Akademie für Sozialwissenschaften das Netz als glaubwürdigste Informationsquelle. Dies ist, so RSF-Asienexperte Brossel, immer mehr eine Illusion. Baidu.com, die größte chinesische Suchmaschine biete z.B. sehr viel politische Webseiten, »aber nirgendwo werden Sie Informationen finden, die der Regierungspropaganda widersprechen« (Rattenhuber SZ 26.01.2006, 12).

China

Identifizierung aller Handy-Nutzenden

Die chinesische Regierung erfasst seit dem 01.01.2006 die persönlichen Daten aller Handy-TelefoniererInnen. Auch die ca. 200 Millionen NutzerInnen von Guthabenkarten müssen sich namentlich anmelden, wenn sie eine neue Karte kaufen. Bisher waren nur die Daten von VertragskundInnen erfasst worden. Gemäß der Ankündigung des Informationsministers Wang Xudong soll mit diesem Schritt der Kriminalität und den Müll-SMS Einhalt geboten werden. Allein im Jahr 2005 seien 10.000 Mobiltelefone wegen des Versendens von erotischen oder betrügerischen Textmitteilungen abgeschaltet worden. Fast jeder Dritte der 1,3 Milliarden ChinesInnen besitzt mittlerweile ein Mobiltelefon (SZ 29.12.2005, 18; KielerN 29.12.2005, 7).

China/Hongkong

Schule verlangt Fingerabdrücke

Um Schulschwänzern schneller auf die Schliche zu kommen, hat sich eine katholische Grundschule in Hongkong jetzt mit digitalen Lesegeräten für Fingerabdrücke gerüstet. Die Jungen und Mädchen müssen vor Unterrichtsbeginn ihre Finger in einen von fünf Apparaten führen, welche die Anwesenheit der SchülerInnen kontrollieren. Die Anlage kostete die Schule auf der Insel Kowloon umgerechnet rund 4.300 Euro und kann auch in der Schulkantine und der Bibliothek zum Einsatz kommen (SZ 12./13.11.2005, 12).

Technik

Mit Laser durch Wände blicken

Im Fachmagazin »Nature Materials« berichtet Chris Phillips vom Imperial College London, dass es ihm mit seiner Forschergruppe grundsätzlich gelungen ist, durch Wände zu sehen. Die Physiker schufen im Labor ein Spezialmaterial aus winzigen Kristallen. Mit einem Laser beschossen wird das normalerweise undurchsichtige Material wie von Zauberhand lichtdurchlässig. »Es entsteht ein rundes Fenster, durch das man hindurchsehen kann«. Dies ist möglich, weil sich die Lichtwellen des Lasers und die Elektronen des Materials ähnlich wie zwei Wellen auf dem Wasser gegenseitig beeinflussen können. Noch lässt sich der Effekt nur mit Spezialmaterial erreichen. Phillips hält es jedoch nur für eine Frage der Zeit, bis der »Röntgenblick« auch normale Türen oder Mauern durchdringen wird: »Wir beginnen zu verstehen, wie Licht mit fester Materie interagiert. Auf Basis dieses Wissens wird es künftig möglich sein, Speziallaser zu entwickeln, die eine Vielzahl von Materialien lichtdurchlässig machen können« (Der Spiegel 9/2006, 138).

Schweiß soll Biometrie sicherer machen

Eine Forschungsgruppe der Clarkson Universität meint eine Lösung dagegen gefunden zu haben, dass sich biometrische Messgeräte für Fingerabdrücke relativ leicht mit Knetmasse überlisten lassen. Sie haben festgestellt, dass die Fehlerquote der Geräte beim Abdruck von schwitzenden Händen nur noch bei 10% liegt. Daher ergänzten die Forschenden das Fingerabdruck-Lesegerät um einen Algorithmus, der nach Schweißspuren sucht; denn die Transpiration folge einem individuellen Schema, das nicht nachgebildet werden könne. Bei einem echten Finger dringe der Schweiß aus einer Pore, breite sich entlang der Hautrillen aus und entwickle so eine eindeutige Prozessstruktur. Die Forscherin Stephanie Schuckers habe nun einen Algorithmus entwickelt, der das Transpirationsmuster entdecke und berücksichtige, wenn ein Fingerabdruck ausgelesen wird: »Da der Nachweis physiologischer Vorgänge die Basis für die Feststellung von Lebenszeichen ist, haben wir angenommen, dass Fingerabdrücke von lebenden Fingern wegen der Transpiration spezifische, sich verändernde Feuchtigkeitsmuster zeigen, gefälschte Fingerabdrücke oder solche von Leichen jedoch nicht« (Omnicard Newsletter Januar 2006, silicon.de).

iTunes spioniert Nutzerverhalten aus

Eine besondere Form unbestellter Überwachung mutet Apple den iTunes-Benutzenden zu. In der neuesten Version (6.02) der Musiksoftware bekommt die HörerIn in einem kleinen Fenster unterhalb ihrer Bibliothek Empfehlungen für Alben im Apples Musicstore, die erstaunlich gut zu dem gerade angehörten Titel passen. Startet man einen MP3 von den Rolling Stones, werden andere Stones-Alben angezeigt sowie Alben von Künstlern, die sich Stones-HörerInnen üblicherweise kaufen. Ganz offensichtlich wird die Information, die Musik welchen Künstlers man gerade hört, an den iTunes-Server übertragen. Dabei spielt es keine Rolle, ob man selbst gerippte MP3s oder gekaufte AAC-Songs hört. Offenbar wird nur der Bandname übertragen – und nicht auch noch das Album und der Songtitel. Zumindest werden diese Daten nicht ausgewertet. Denn sobald man

den Bandnamen im ID-Tag verändert, werden die bandbezogenen Tipps aus dem Apple-Store durch allgemeine Werbung ersetzt.

In Blogs wird zudem berichtet, dass die Übertragung der Bandinformation sofort unterbleibt, wenn man das Mini-Storefenster abschaltet. Diese Erkenntnis soll sich aus der Analyse der Netzwerktraffics ergeben. Nach der Installation der neuen iTunes-Version ist das Mini-Storefenster jedoch standardmäßig eingeschaltet. Die Übertragung selbst der Bandinformation ist aus Datenschutzsicht nicht zu rechtfertigen. Eine explizite Zustimmung, dass Apple einen Blick in der eigene MP3-Sammlung wirft und das Nutzerverhalten auswertet, wird von den Nutzenden nicht eingeholt (Dambeck www.spiegel.de 11.01.2006).

Hilferuf per Handy

Kamera-Handys sollen es künftig Opfern von Entführungen oder Gewaltverbrechen ermöglichen, heimlich um Hilfe zu rufen. Der Handy-Hersteller Nokia hat in den USA ein Notfallsystem für Mobiltelefone zum Patent angemeldet, das per Knopfdruck das Versenden eines Notrufes inklusive zeitnah aufgenommener Fotos, Filme und Töne ermöglichen soll. Werden zwei in das Gerät integrierte Panikknöpfe gleichzeitig für eine bestimmte Zeit gedrückt, verschickt das Handy zunächst eine zuvor aufgezeichnete Sprachnachricht. Anschließend fotografiert oder filmt die Handy-Kamera die Umgebung. Zusammen mit dem über ein Mikrofon aufgenommenen Ton und der per GPS bestimmten Position der Geräts werden diese Daten dann an einen zuvor bestimmten Empfänger versandt. Das System soll selbst bei ausgeschaltetem Handy aktivierbar sein. Ist gerade kein Netz vorhanden, werden die Daten gespeichert und automatisch versandt, sobald dies wieder möglich ist.

Derweil ergab eine Studie, für die im Auftrag der britischen Telekommunikationsfirma Virgin Mobile 2.000 Menschen befragt wurden, dass für viele Menschen ein Leben ohne Handy zu einer beängstigenden Vorstellung geworden ist. Die überwiegende Mehrheit der Befragten fühlt sich danach schon bei kurzer Trennung vom Mobiltelefon unter Stress gesetzt. 90% der Teilnehmer gaben an, mindestens einmal pro Stunde ihr Handy zu nutzen. Vier von fünf Befragten fühlten sich unwohl, wenn ihr Telefon für längere Zeit nicht in Reichweite war. 84% gaben an, sie würden ihr Handy nie aus den Augen lassen (Der Spiegel 4/2006, 151; SZ 27.01.2006, 12).

Sinnvolle RFID-Anwendungen im Strafvollzug?

In einer vom Verband für Sicherheitstechnik veranstalteten Forensik-Tagung in Nürnberg wurde im Januar 2006 über den Einsatz von RFID-Chips bei der Überwachung von Psychiatriepatienten und Straftätern im Strafvollzug diskutiert. Stephan Baumann, Professor für Verkehrsnachrichtensysteme an der TU Dresden betreibt in Kooperation mit der RWTH Aachen das Projekt Sm@rt Logistics. Er erklärte Transponder, Kommunikationsprotokolle und Einsatzgebiete. Sie reichen vom Kanban-System in der Logistik bis zu einem System, das Museumsbesucher sowie Ausstellungsstücke mit RFID-Tags überwacht. Anders als in Hessen, wo seit fünf Jahren ein Funkfesselsystem im Einsatz ist, arbeitet ein Österreichisches System mit RFID. Ziel aller Systeme sei dabei nur die Beachtung des Hausarrestes. Dem gegenüber ermöglicht ein Produkt der Firma Alanco Technologies eine umfassende Kontrolle von Menschen z.B. in Gefängnisanstalten. Baumann schloss mit dem Fazit: »RFID-Anwendungen erscheinen im Bereich des Strafvollzugs durchaus sinnvoll.« Zu ihrer Realisierung müssten zuvor juristische, ethische, betriebswirtschaftliche und technische Fragen geklärt werden (Borchers www.heise.de 26.01.2006).

Gentechnik

USA

Gentest klärte erstmals Schuld von Hingerichtetem

Erstmals in der Geschichte der Todesstrafe in den USA hat der Gouverneur eines Bundesstaates einen Gentest im Fall eines als Mörder hingerichteten Mannes angeordnet. Virginias scheidender Gouverneur Mark Warner ließ überprüfen, ob der 1992 als Sexualmörder hingerichtete Roger K. Coleman Opfer eines Justizirrtums wurde. Coleman hatte seine Unschuld noch kurz vor seinem Tod mit den Worten beteuert: »Hier wird ein unschuldiger Mann ermordet. Wenn meine Unschuld erwiesen ist, hoffe ich, dass Amerika das Unrecht der Todesstrafe erkennt – so wie alle anderen zivilisierten Länder.« Warner, ein konservativer Demokrat, hatte kurz vorher einen zum Tod verurteilten Mann begnadigt, über dessen Schuld letzte Zweifel nicht ausgeräumt waren. Warner hatte im Dezember 2005 zudem die Überprüfung tausender Urteile aus den 70er und 80er Jahren angeordnet, nachdem eine Untersuchung von 31 zum Teil jahrelang zurückliegenden Kriminalfällen zur sofortigen Freilassung zweier wegen Vergewaltigung verurteilter Männer geführt hatte. Die neuen Gentests hatten unzweifelhaft nachgewiesen, dass sie jahrelang zu Unrecht im Gefängnis saßen.

Es hatte nicht sein sollen, dass diese Maßnahme zu einem Signal gegen die Todesstrafe in den USA würde: Die Genuntersuchung zeigte, dass die Spermaspuren am Körper der ermordeten 19-jährigen Wanda McCoy von dem hingerichteten Coleman stammten. Die christliche Gefangenen-Hilfsorganisation »Centurion Ministries« hatte sich nach der Hinrichtung für den DNS-Test eingesetzt. Deren Direktor, James McCloskey, meinte, das Testresultat sei bitter. Bisher ist es in den USA noch nie vorgekommen, dass nach einer Hinrichtung die Unschuld eines Exekutierten wissenschaftlich nachgewiesen wurde. Allerdings wird erwartet, dass der Test in Virginia ähnliche Untersuchungen nach sich zieht. Der Demokrat Warner wird als Kandidat für die Präsidentschaftswahl 2008 gehandelt (Klüver SZ 07./08.01.2006, 8; SZ 14./15.01.2006, 11).

Rechtsprechung

BGH

Keine schriftliche Dokumentationspflicht bei Anlageberatung

Nach einem Urteil des Bundesgerichtshofes (BGH), das am 24.01.2006 veröffentlicht wurde, müssen Bankangestellte bei Beratungsgesprächen mit Kapitalanlegern keine umfassende schriftliche Dokumentation vornehmen. Die Richter des 11. Senats gaben damit der Dresdner Bank recht, die von einer ihrer Kundinnen wegen eines angeblichen Beratungsfehlers verklagt worden war. Trotz ihres konservativen Anlageverhaltens habe die Bank zur Umschichtung ihrer Wertpapierdepots auf hochspekulative Multimedia-, Biotechnologie-, Software- und Internetfonds geraten, behauptete die Klägerin, die durch die Umschichtung erhebliche Kursverluste hinnehmen musste. Inhalte des Gesprächs wurden nicht notiert. Bereits die Vorinstanzen hatten die Klage abgewiesen (Az. XI ZR 320/04; SZ 25.01.2006, 26).

BVerfG

Für die Zukunft: präventiver Persönlichkeitsschutz geht vor Äußerungsfreiheit

Der frühere Bundesverkehrsminister Manfred Stolpe darf künftig nicht mehr als Stasi-Mitarbeiter bezeichnet werden. Das Bundesverfassungsgericht (BVerfG) hob ein anders lautendes Urteil des Bundesgerichtshofes (BGH) aus dem Jahr 1998 auf und stärkte damit den Persönlichkeitsschutz. Der BGH sei den hohen Anforderungen an die Wahrheitspflicht nicht gerecht geworden, die für unbewiesene Tatsachenbehauptungen und bei schwerwiegenden Eingriffen in das Persönlichkeitsrecht gelten. Eine umstrittene oder zweifelhafte Tatsache dürfe nicht einfach als feststehend hingestellt werden.

Der VI. BGH-Senat muss sich nun in anderer Besetzung als 1998 erneut mit einem Ausspruch des CDU-Politikers Uwe Lehmann-Brauns befassen. Der hatte im April 1996 in einer ZDF-Sendung behauptet, »dass Herr Stolpe, wie wir alle wissen, über 20 Jahre im Dienste der Staatssicherheit tätig« gewesen sei. Als Vertreter der evangelischen Kirche unterhielt Stolpe von 1969 bis 1989 Kontakte zu hauptamtlichen Mitarbeitern des DDR-Ministeriums für Staatssicherheit. Dieses hatte ihn unter der Bezeichnung »IM Sekretär« als inoffiziellen Mitarbeiter geführt. Stolpes Stasi-Kontakte sowie eine DDR-Verdienstmedaille für ihn waren nach der Wende Gegenstand zahlreicher politischer und juristischer Auseinandersetzungen. Im Vorfeld der Volksabstimmung über die Vereinigung der Bundesländer Berlin und Brandenburg fiel die Äußerung des Berliner CDU-Politikers, der wegen Stolpes Vergangenheit nicht dessen Landeskind werden wollte – wie er sagte.

Stolpe erhob daraufhin Unterlassungsklage. Die Tatsachenbehauptung, er sei über 20 Jahre im Dienste der Stasi tätig gewesen, sei falsch und eine Verleumdung seiner Person. Er sei niemals Inoffizieller Mitarbeiter des Stasi-Ministeriums gewesen. Das Oberlandesgericht Brandenburg entschied für Stolpe, der BGH gegen ihn. Die Äußerung lasse verschiedene Deutungsmöglichkeiten, so der BGH. Es müsse außerdem zwischen Meinungsfreiheit und Ehrenschutz abgewogen werden. Dem Recht auf freie Äußerung gebühre, so der BGH, der Vorrang. Der Angriff auf Stolpe sei im öffentlichen Meinungskampf gefallen, und zwar, als es um eine Frage ging, die die Allgemeinheit wesentlich berühre.

Das BVerfG widersprach der Abwägung des BGH in seinem 28-seitigen Grundsatzbeschluss. Der BGH habe Maßstäbe zu Grunde gelegt, die aus guten Gründen für mehrdeutige Meinungsäußerungen in der Vergangenheit entwickelt worden sind. So müsse sich der Staat mit Sanktionen wie Strafe, Schadensersatz oder Widerruf zurückhalten, wenn es um frühere Äußerungen gehe. Andernfalls könnte eine staatliche Sanktion »wegen ihrer einschüchternden Wirkung die freie Rede, freie Information und freie Meinungsbildung empfindlich berühren«. Anders bewertete das BVerfG hingegen erstmals das Verhältnis von Meinungsfreiheit und Persönlichkeitsrecht bei künftigen Äußerungen, auf die ein Unterlassungsanspruch wie derjenige von Stolpe zielt. Hier sei kein Einschüchterungseffekt zu erwarten, weil sich jeder vorher den Inhalt einer Äußerung gut überlegen könne. In solchen Fällen könne man Verletzungen des Persönlichkeitsrechts ohne weiteres vermeiden. So müsse bei der Verbreitung konkreter Behauptungen der Hinweis verlangt werden, dass eine bestimmte Sicht der Dinge umstritten und der fragliche Sachverhalt nicht wirklich aufgeklärt sei (Az. 1 BvR 1696/98; SZ 17.11.2005, S. 6).

BayVerfGH

Durchsuchungen bei Schleierfahndung eingegrenzt

Der Bayerische Verfassungsgerichtshof (BayVerfGH) hat der umstrittenen Schleierfahndung (vgl. DANA 1/2005, 21) Grenzen gesetzt. Bei Kontrollen im Rahmen der Schleierfahndung sind danach willkürliche Untersuchungen persönlicher Gegenstände durch die Polizei nicht zulässig, es sei denn, es gäbe Hinweise auf »eine erhöhte abstrakte Gefahr«. Dies bedeute insbesondere, dass solche Durchsuchungen nicht auf Grund einer ungesicherten oder nur diffusen Tatsachenbasis erfolgen dürfen.

Mit seinem Urteil hat das Gericht der Verfassungsbeschwerde eines Bürgers aus Schwaben stattgegeben, dessen Wagen am 10.04.2002 von einer Polizeistreife gründlich durchsucht worden war - bis hin zur Visitenschachtel. Das Misstrauen der Beamten war geweckt worden, weil der Mann einen über 30 Jahre alten altersschwachen Mercedes fuhr und einen ausländischen Beifahrer im Auto hatte. Die Polizisten vermuteten, bei den beiden kontrollierten Personen handele es sich um Drogendealer.

Der BayVerfGH befand, dass Ausweiskontrollen durchaus hinnehmbar seien. Eine Durchsuchung mitgeführter Sachen sei aber ein »deutlich schwerwiegenderer Eingriff«. Wenn die Polizei auch ohne Hinweise auf eine erhöhte Gefahr Gepäck und persönliche Sachen durchsuchen dürfte, könnte jeder Bürger auf der Autobahn einer Durchsuchung ausgesetzt sein: »Damit wären potenziell breite Kreise der Bevölkerung von dieser weit reichenden Eingriffsmöglichkeit betroffen.« Es müsse ein Ausgleich zwischen den Interessen der Bürger und der Polizei gefunden werden. Einerseits müsse es eine wirksame Einschreitschwelle geben; andererseits müsse aber gewährleistet werden, dass nicht beliebig viele Personen von dem schwerwiegenden Eingriff einer Durchsuchung betroffen würden. Mit seiner Entscheidung wurde eine vorangegangene verwaltungsgerichtliche Entscheidung aufgehoben. Das Verwaltungsgericht Augsburg muss sich erneut mit der Klage des Bürgers befassen.

Sowohl die Grünen als auch die SPD begrüßten das Urteil ausdrücklich. Nun müsse Innenminister Günther Beckstein für eine entsprechende Klarstellung im Polizeiaufgabengesetz sorgen. Bereits 2003 hatten die Grünen vor dem BayVerfGH gegen die grenzenlose Schleierfahndung geklagt, waren damals aber unterlegen. Durch das jüngste Urteil sehen sie sich nun in ihrer Kritik bestätigt. Grünen-Abgeordnete Christine Stahl: »Der unsäglichen Jedermannkontrolle ohne Anlass ist nun endlich ein Riegel vorgeschoben.« Das Innenministerium erklärte zu dem Urteil, dieses »wirkt sich auf die heutige polizeiliche Praxis kaum aus«. Die Schleierfahndung ist 1995 in Bayern in Kraft getreten. Nach dem Wegfall der EU-Binnengrenzen soll sie die bis dahin üblichen Grenzkontrollen ersetzen (Schneider SZ 10.02.2006, 1, 30; vgl. DANA 2/1997, 27).

BAG

Lohnfortzahlung nur nach Schweigepflichtentbindung

Das Bundesarbeitsgericht (BAG) entschied in einem Urteil, dass Arbeitnehmer, die in kurzen Abständen aus unterschiedlichen Gründen krank geschrieben werden, ihren Arzt von der Schweigepflicht entbinden müssen, um die Lohnfortzahlung zu sichern (Az. 5 AZR 389/04). Der Arbeitnehmer müsse beweisen, dass es sich um eine neue und nicht um eine Fortsetzungskrankheit handele. Das BAG gab damit seine bisherige Rechtsprechung auf. Als Fortsetzungserkrankung gilt eine Arbeitsunfähigkeit, die »auf demselben nicht behobenen Grundleiden beruht«. Dabei ist es egal, ob sich das Grundleiden wieder in seiner ursprünglichen Form oder neuartig äußert. Tritt eine solche Fortsetzungserkrankung nach weniger als sechs Monaten auf, so werden beide Arbeitsunfähigkeiten zusammengelegt und die Lohnfortzahlung bleibt auf insgesamt sechs Wochen beschränkt. Dagegen muss der Arbeitgeber erneut Lohnfortzahlung für bis zu sechs Wochen leisten, wenn die Arbeitunfähigkeit auf einer neuen Krankheit beruht (SZ 07./08.01.2006, V1/11).

OVG Rheinland-Pfalz

Polizeischutz-Überwachung für Nachbarn verhältnismäßig

Das Oberverwaltungsgericht (OVG) in Koblenz hatte darüber zu entscheiden, ob die Überwachungs- und Kontrollmaßnahmen, die seit sieben Jahren zum Zweck des Polizeischutzes eines Oberstaatsanwaltes in der rheinland-pfälzischen Stadt stattfinden, von den Nachbarn zu erdulden sind. Jeden Morgen holt eine Polizeieskorte den Mann, der in einem Mehrfamilienhaus wohnt, ab. Dort sind Kameras installiert. Die Besucher werden kontrolliert, manchmal auch die Bewohner selbst. Der Oberstaatsanwalt ist für Organisierte Kriminalität zuständig; geschützt wird er, seit im April 1999 ein Mordauftrag gegen ihn bekannt wurde. Als Motiv dafür gilt Rache, mit der Folge, dass auch ein Wechsel der Funktion die Gefahr nicht reduzieren würde. Die Mitbewohner schätzen wenig den Kollateralnutzen der Überwachung, z.B. ohne Angst vor Einbrechern verreisen zu können. Sie hatten schon Einiges auszuhalten. Vor zwei Jahren stürmte z.B. ein Sondereinsatzkommando das Haus, weil irrtümlich ein Anschlag gemeldet worden war.

Eine Mitbewohnerin klagte erfolglos auf eine Ende der Überwachung. Hilfsweise regte sie den Umzug an, am besten in ein frei stehendes Einfamilienhaus. Dort sei der Oberstaatsanwalt besser zu schützen. Das OVG meinte dagegen, die Überwachung sei verhältnismäßig: »Die Einschränkungen für den Staatsanwalt und seine Frau gehen weit über das hinaus, was die Mitbewohner hinzunehmen haben.« Ein Wohnungswechsel sei dem Ermittler nicht zuzumuten, zumal das Problem nur verlagert werde; auch würde dessen »soziale Isolierung« dadurch weiter verstärkt. Die Mitbewohnerin prüft, ob sie Beschwerde beim Bundesverwaltungsgericht einlegen soll.

Die Nachbarschaft zu einer gefährdeten Person ist oft eine zwiespältige Angelegenheit. In Hannover schaltete eine Kauffrau, die gegenüber des damaligen Bundeskanzlers Gerhard Schröder ein Lebensmittelgeschäft betreibt, einen Anwalt ein, um Parkplätze für ihre Kunden zu erhalten. In Eltville am Rhein wiederum hofft man, dass sich mit der Ernennung des Mitbürgers Franz Josef Jung zum Verteidigungsminister Pläne erledigt haben, die örtliche Polizeistation zu schließen (Esslinger SZ 03.01.2006, 6).

Hessischer VGH

Akteneinsicht für Flughafen-Ausbaugegner

Der Hessische Verwaltungsgerichtshof (VGH) verpflichtete das Regierungspräsidium Darmstadt, Ausbaugegnern des Frankfurter Flughafens Einsicht in die verwaltungsinternen Akten zu geben. Vier Ausbaukritiker aus dem Frankfurter Stadtteil Sachsenhausen hatten geklagt und sich auf die EU-Umweltinformationsrichtlinie berufen. Sie verlangten Einsicht in die Planunterlagen, die nicht öffentlich ausgelegt waren. Hierzu gehören die Stellungnahmen der Fachbehörden sowie ergänzende Gutachten zum Ausbauprojekt der Fraport. Die Behörde hatte die Einsicht verweigert. Die Unterlagen würden derzeit vervollständigt und beträfen verwaltungsinterne Vorgänge; außerdem behindere die Akteneinsicht die zügige Abwicklung des Erörterungsverfahrens. Der VGH widersprach dieser Auffassung. Nach der EU-Richtlinie müsse die Öffentlichkeit einen generellen Zugang zu Umweltinformationen erhalten (FR 07.01.2006, 23).

LG Darmstadt

Verbindungsdatenspeicherung nur für Rechnungszwecke

Die T-Online AG muss die IP-Adressen von Flatrate-Nutzenden sofort nach Beendigung der jeweiligen Verbindung löschen. So urteilte am 25.01.2006 das Landgericht (LG) Darmstadt in zweiter Instanz (Az. 25 S 118/2005). Das bislang mitgespeicherte Volumen darf der Provider nicht einmal erheben, geschweige den speichern, da diese Daten für die Rechnungsstellung nicht erforderlich sind und deshalb nach dem Telekommunikationsgesetz (TKG) nicht verarbeitet werden dürfen. Geklagt hatte Holger Voss, der Anfang 2003 wegen eines satirischen Beitrages in einem Forum des zum Heise Zeitschriften Verlag gehörenden Online-Magazins Telepolis angeklagt und freigesprochen worden war. Anlässlich dieses Verfahren erwies sich, dass T-Online die dem Kunden zugewiesenen IP-Adressen bis zu 80 Tage nach Rechnungslegung in Verbindung mit den Bestandsdaten speichert. Solange können damit auch die Ermittlungsbehörden mit einem richterlichen Beschluss die Herausgabe dieser Daten erwirken.

Schon das Amtsgericht Darmstadt hatte in erster Instanz Anfang Juli 2005 entschieden (Az. 300 C 397/04), dass die Speicherung von IP-Adressen bis 80 Tage nach Rechnungsstellung den Datenschutzbestimmungen widerspreche. Das Amtsgericht hatte es aber für vertretbar angesehen, wenn es mehrere Tage dauert, bis die Daten gelöscht werden. Auch störte Voss, dass nach dem AG Darmstadt T-Online speichern dürfe, wann und wie lange er ins Internet eingewählt war und welche Datenmengen er dabei empfangen und versendet hat.

Der Berufung von T-Online gab das LG nicht statt. Allerdings darf das Unternehmen zu Rechnungszwecken die Daten über Beginn und Ende der Verbindung bis zu acht Wochen aufbewahren, weil die Flatrate »nicht völlig flat« sei. Gemäß den Vertragsbedingungen von T-Online werden nämlich dann Kosten fällig, wenn sich der Kunde statt über DSL über die im Vertrag ebenfalls vorgesehene Möglichkeiten Analog-Modem, ISDN-Anschluss oder Mobiltelefon einwählte. Dann werde ein zeitabhängiges Entgelt berechnet.

Datenschützer begrüßten das Urteil, so Johann Bizer vom Unabhängigen Landeszentrum für Datenschutz Schleswig-Holstein: »Das Urteil stellt eine Herausforderung dar, seine Server auf ein datenschutzfreundlicheres Verfahren der Abrechnung umzustellen.« T-Online sieht dagegen in dem Urteil keinen Präzedenzfall, wie Martin Frommhold darstellt: »Das gilt nur für diesen individuellen Kunden.« Sollten andere Kunden darauf bestehen, dass ihre Daten ebenfalls gelöscht werden, müssten sie das per Gericht durchsetzen. »Die für uns zuständige Aufsichtsbehörde hält die Speicherung der IP-Adresse bei Flatrates aber nach wie vor für zulässig« (Ermert www.heise.de 25.01.2006; Schrader SZ 26.01.2006).

LG Flensburg

Keine Strafanzeigen-Maschinerie wegen Urheberrechtsverstößen

Der schweizer Dienstleister Logistep darf Internetprovider im Kampf gegen Urheberrechtsverstöße durch Tauschbörsen-Nutzende nicht mehr massenhaft zur Speicherung von Verbindungsdaten anhalten. Nach einem Urteil des Landgerichts (LG) Flensburg vom 25.11.2005 ist bei Anwendung der Haftungsregeln im Teledienstegesetz (TDG) der Zugangsanbieter für fremde Inhalte grundsätzlich nicht verantwortlich und deshalb auch nicht verpflichtet, seine KundInnen zu überwachen oder nach Umständen für eine rechtswidrige Nutzung ihrer Dienste zu suchen. Wird ein Provider über das illegale Treiben von Kunden in Kenntnis gesetzt, gilt er fortan zwar als »Störer« und kann zum Eingreifen verpflichtet sein. Diese Haftung begründet aber, so das LG Flensburg, keine Auskunftsansprüche gegenüber dem Anbieter, sondern allein einen Unterlassungsanspruch. Eine Pflicht zur Mithilfe zum Erwirken von Schadenersatz bestehe nicht. »Unter keinem rechtlichen Gesichtspunkt« könne von einem Zugangsanbieter verlangt werden, »irgendwelche Daten oder Informationen zu speichern«.

Das Urteil könnte Präzedenzwirkung haben für andere Provider, sich gegen den Kläger Logistep und dessen Massenmails zur Wehr zu setzen. Logistep setzte im Sommer 2005 im Auftrag der Karlsruher Kanzlei Schutt-Waetke eine Strafanzeigen-Maschinerie in bis dahin unbekannter Dimension in Gange. Logistep hat eine spezielle Software entwickelt, mit der sie die Anbieter urheberrechtswidrig verbreiteter und veröffentlichter Werke wie PC-Spiele, Musikstücke oder Videos aufspüren und die IP-Adresse zum Zeitpunkt der Rechtsverletzung festhalten kann. Mit Hilfe dieser Informationen kann über den jeweiligen Provider die Identität des Nutzers hinter der Netzadresse ermittelt werden. Das Hauptinteresse der selbst ernannten Raubkopiererjäger liegt bislang beim Spiel Earth 2160 des Karlsruher Herstellers Zuxxez Entertainment. Wie die Staatsanwaltschaft Karlsruhe bestätigte, sind dort mit Hilfe Logisteps allein im Juni und Juli 2005 über 20.000 Strafanzeigen wegen Urheberrechtsverletzung eingegangen.

Die schweizer Firma versucht ihre Anzeigen-Automatik dadurch zu verbessern, dass sie Provider mit automatisch generierten Nachrichten zur Speicherung der jeweiligen Verbindungsdaten auffordert. Zuvor hatten sie die Erfahrung gemacht, das gerade Flatrate-Anbieter die begehrten Informationen für eigene Abrechnungszwecke nicht benötigen und daher rasch löschen. Versatel erhielt auf diese Weise innerhalb von 14 Tagen 507 entsprechende Emails von Logistep, davon allein an einem Tag 167 Mails, was dem Anbieter zufolge zu einer Blockierung seiner Server führte. Die frankfurter Anwaltskanzlei Schalast&Partner erwirkte daraufhin im August 2005 eine einstweilige Verfügung, in der Logistep die ungewöhnliche Speicheranmahnung untersagt wurde. Die schweizer Firma legte daraufhin Widerspruch ein, den das flensburger Gericht in seiner Entscheidung auf Grund des erfolgten Eingriffs in der Gewerbebetrieb von Versatel zurückwies (Krempl www.heise.de 15.12.2005).

Buchbesprechungen



Gola, Peter/Jaspers, Andreas

Das BDSG im Überblick

Datakontext Fachverlag Frechen, 3. Aufl. 2006, 88 S., 24 Euro, ISBN 3-89577-376-X

(tw) Die »Erläuterungen, Schaubilder und Organisationshilfen zum BDSG für die Datenschutzpraxis«, herausgegeben in Zusammenarbeit mit der Gesellschaft für Datenschutz und Datensicherheit e.V. (GDD), sind ein brauchbares Einsteiger-Set zum BDSG. Die als Broschüre gestaltete Schrift bietet in kleinen Portionen die wesentlichen Inhalte des BDSG zum Eigenstudium sowie zur Ausbildungsbegleitung. Sie schafft es, das teilweise nicht gerade unkomplizierte Gesetzeswerk einfach verständlich an den Menschen zu bringen, der sich mit dem BDSG – freiwillig oder unfreiwillig – ein wenig auskennen muss. Für den betrieblichen Datenschutzbeauftragten mag es die allererste Einstiegshilfe sein, aber auch nicht mehr. Die Kurzerläuterungen zu wichtigen Regelungen, die Schaubilder, die Formularvordrucke erleichtern, aber ersetzen nicht den Blick in das Gesetz, das am Ende abgedruckt ist, und schon gar nicht den Blick in den Kommentar bei konkreten praktischen Konfliktlagen und Fragen. Die Muster für ein Mitarbeiter-Merkblatt, für eine betriebliche Datenschutzrichtlinie, einer Checklist zur Umsetzung der »8 Gebote« nach § 9 BDSG und einer Stellenbeschreibung des betrieblichen Datenschutzbeauftragten sind – in die Praxis umgesetzt – mehr als was üblicherweise in einem kleinen oder mittleren Unternehmen an Datenschutz vorgefunden werden kann. Aber es genügt nicht, wenn mehr als nur die Form des Datenschutzes eingehalten werden soll. Also: sehr geeignet als Einstieg für den bDSB, gut als Ausbildungsmaterial für Mitarbeiter. Wer Hinweise auf Spezialprobleme sucht, auf Literatur, auf soziale, ökonomische oder rechtliche Hintergründe, der muss andere weitergehende Literatur heranziehen.



Gola, Peter

Datenschutz und Multimedia am Arbeitsplatz

Datakontext Fachverlag, Frechen 2006, 208 S., 39,00 Euro, ISBN 3-89577-360-3

(tw) Wer einen umfassenden Überblick über Datenschutz für Arbeitnehmer am Arbeitsplatz bei der Nutzung von Kommunikationstechnik haben möchte, dem kann dieses Buch sehr empfohlen werden. Der Autor arbeitet das Thema unter umfassender Auswertung der verfügbaren Literatur auf. Dabei zieht er auch die Tätigkeitsberichte der Datenschutzbehörden wie auch gewerkschaftlich orientierte Literatur heran. Neben dem klassischen Datenschutzrecht befasst sich das Buch auch mit den relevanten Nebengesetzen, z.B. dem Strafgesetzbuch, dem Kunsturhebergesetz, dem Telekommunikations- und dem Multimediarecht. Behandelt werden nicht nur individuell-rechtliche, sondern auch Mitbestimmungs-Fragen. Alle denkbaren Fallkonstellationen werden kurz, aber äußerst prägnant behandelt, vom Einsatz von Telefon, Handy, Internet, Email, Video, RFID... Durch die Behandlung moderner Arbeitsplatzüberwachungstechniken befindet sich die Darstellung auf der Höhe der Zeit. Die Besonderheit spezieller Berufe – also von Schweigepflichtigen oder Schweigeberechtigten vom Journalisten über den Richter bis zum Arzt – werden angesprochen. Auch konventionelle Kontrollformen wie das direkte Mithören oder Mystery Calls werden behandelt. Nicht thematisiert werden allgemeine Kontrollfragen, z.B. des betrieblichen Datenschutzbeauftragten oder der Aufsichtsbehörde, soweit es hierzu keine arbeitsplatzspezifischen Besonderheiten gibt.

Die Positionen des Autors sind durchgängig gut begründet und ausgewogen. Er nimmt nicht eindeutig Position für die Arbeitnehmer- oder die Arbeitgeberseite, sondern sucht einen Ausgleich. Man muss nicht in jeder behandelten Einzelfrage dem Autor zustimmen. Seine Position hindert ihn nicht, auch abweichende Meinungen umfassend darzustellen und evtl. gar ausführlich per Zitat zu Wort kommen zu lassen, so dass sich die Leserin bzw. der Leser ein eigenes Bild machen kann. Die vorhandene Rechtsprechung wird referiert. Dadurch ist i.d.R. ein Rückgriff auf weitere Literatur überflüssig. Ein Schwergewicht wird gelegt auf den Datenschutz bei Call-Center-Arbeitsplätzen, wobei Vorarbeiten eines Buches zu diesem Thema in die nunmehr umfassendere Darstellung eingeflossen sind, ohne dass dortige Mängel übernommen wurden (vgl. DANA 1/2002, 22). Abgerundet wird das Buch durch gut brauchbare Inhalts-, Literatur- und Stichwortverzeichnisse, die auch das selektive Suchen nach Antworten auf spezielle Fragen erleichtern. Alles in allem: Zum Thema Arbeitnehmerdatenschutz ein sehr zu empfehlendes Standardwerk.

Widerstand gegen geplante Vollprotokollierung der Telekommunikation

Gemeinsame Erklärung von Datenschützern, Journalisten und Verbraucherzentrale: »Datenspeicherung ist inakzeptabel«

Berlin, 07.02.2006 – In einer gemeinsamen Erklärung sprechen sich Datenschützer, Verbraucherschützer und Journalisten gegen die von der Bundesregierung befürwortete Vorratsspeicherung von Telekommunikationsdaten aus. EU-Pläne sehen vor, dass künftig jede Benutzung von Telefon, Handy und Internet protokolliert werden soll, damit Strafverfolgungsbehörden auf diese Informationen zugreifen können. Nachdem das Europäische Parlament im Dezember grünes Licht gab, haben die EU-Justizminister dem Regelungsvorschlag im Februar zugestimmt (vgl. S. 17 ff.).

Zehn Verbände, darunter der Verbraucherzentrale Bundesverband (vzbv), der Deutsche Journalisten-Verband (DJV) und der Chaos Computer Club CCC), bezeichnen die geplante Datenspeicherung als inakzeptabel.

»Sie bewirkt keinen verbesserten Schutz vor Kriminalität, kostet Millionen von Euro, gefährdet die Privatsphäre und die Sicherheit Unschuldiger, beeinträchtigt vertrauliche Kommunikation und ebnet den Weg in eine immer weiter reichende Massenüberwachung der Bevölkerung«, heißt es in der gemeinsamen Erklärung der Verbände. Die Vereinbarkeit einer Vorratsdatenspeicherung mit den Grundrechten solle gerichtlich überprüft werden.

Der Verbraucherzentrale Bundesverband (vzbv) sieht in den Plänen zur Vorratsdatenspeicherung eine Bedrohung des Rechts auf informationelle Selbstbestimmung. »Eine demokratische Gesellschaft zeichnet sich dadurch aus, dass nicht der Staat die Bürger, sondern die Bürger den Staat kontrollieren«, so vzbv-Vorstand Prof. Dr. Edda Müller. Eine verdachtsunabhängige Vorratsdatenspeicherung bedeute den Einstieg in eine flächendeckende Überwachung der Nutzer digitaler Kommunikation. Das Prinzip der informationellen Selbstbestimmung drohe zunehmend zu einem Grundsatz der informationellen Fremdbestimmung zu werden.

Die zehn Verbände fordern die Mitglieder des Bundestags auf, an ihrer 2005 erklärten Ablehnung der Massendatenspeicherung festzuhalten.

Falls die EG-Richtlinie nicht zu verhindern sei, müssten wenigstens die verbleibenden Spielräume zugunsten der Bürger und der Wirtschaft voll ausgeschöpft werden. Die Organisationen präsentieren einen Zehn-Punkte-Forderungskatalog zur nationalen Umsetzung der Richtlinie. So soll die Datenspeicherung und der Datenabruf auf ein Minimum beschränkt werden. Die bestehende Identifizierungspflicht vor dem Abschluss von Telefon-und Handyverträgen soll aufgehoben werden.

Weitere Punkte sind:

- Die Ausschöpfung der maximalen Umsetzungsfrist bis Mitte 2007 – für Internetdaten bis Anfang 2009.
- Eine Vorratsdatenspeicherung nur für die in der Richtlinie genannten Datentypen und nur für die Dauer von sechs Monaten.
- Die Zulässigkeit des Zugriffs auf die Kommunikationsdaten nur zur Verhinderung oder Verfolgung schwerer Straftaten, wenn im Einzelfall der konkrete Verdacht einer solchen Tat besteht.
- Den Zugriff auf und die Verwertung von Informationen über die Kommunikation von Ärzten, Rechtsanwälten, Steuerberatern, anderen Berufsgeheimnisträgern sowie Journalisten nur in Ausnahmefällen zuzulassen.

Die Erklärung im Wortlaut:

Gemeinsame Erklärung zur Vorratsdatenspeicherung in Deutschland

Die systematische Aufzeichnung und Aufbewahrung von Informationen über die Kommunikation, Bewegungen und Mediennutzung der gesamten Bevölkerung (»Vorratsdatenspeicherung«) ohne Einwilligung der Betroffenen ist inakzeptabel. Sie bewirkt keinen verbesserten Schutz vor Kriminalität, kostet Millionen von Euro, gefährdet die Privatsphäre und die Sicherheit Unschuldiger, beeinträchtigt vertrauliche Kommunikation und ebnet den Weg in eine immer weiter reichende Massenüberwachung der Bevölkerung.

Wir fordern, Vorratsspeicherungspflichten von den deutschen und europäischen Gerichten auf ihre Vereinbarkeit mit den Grundrechten hin überprüfen zu lassen.

Die Abgeordneten des Deutschen Bundestags fordern wir auf, an ihrer Ablehnung einer verdachtslosen Vorratsdatenspeicherung festzuhalten und stattdessen weniger eingreifende Alternativen zu prüfen (z.B. das »Quickfreeze«-Verfahren).

Für den Fall, dass der Deutsche Bundestag eine EG-Richtlinie zur Vorratsdatenspeicherung trotz allem umsetzen sollte, fordern wir:

1. Die maximale Umsetzungsfrist bis Mitte 2007 – für Internetdaten bis Anfang 2009 – ist auszuschöpfen.
2. Bürger dürfen nicht verpflichtet werden, sich vor der Nutzung von Telefon, Handy oder Internet zu identifizieren. Bestehende Identifizierungspflichten sind aufzuheben.
3. Eine Vorratsspeicherung wird nur für die in der Richtlinie genannten Datentypen und nur für die Dauer von sechs Monaten eingeführt; danach sind die Daten unverzüglich zu löschen. Zu speichern sind nur Daten, die bei dem jeweiligen Anbieter zur Bereitstellung von Kommunikationsdiensten ohnehin erzeugt oder verarbeitet werden.
4. Der Staat hat die zur Datenspeicherung und -vorhaltung verpflichteten Anbieter für die daraus resultierenden Zusatzkosten (Investitionskosten, Vorhaltekosten, Personalkosten) voll zu entschädigen.
5. Der staatliche Zugriff auf Informati-

onen über die Kommunikation und die Kommunizierenden (»Verkehrsdaten«, »Bestandsdaten«) hat den gleichen Voraussetzungen zu unterliegen wie der Zugriff auf die Inhalte der Kommunikation.

6. Der Zugriff auf Kommunikationsdaten ist nur zur Verhinderung oder Verfolgung schwerer Straftaten zuzulassen, wenn im Einzelfall der konkrete Verdacht einer solchen Tat besteht. Der Zugriff zwecks Strafverfolgung sollte beschränkt sein auf Fälle organisierter Kriminalität, in denen eine höhere Strafe als vier Jahre Freiheitsstrafe zu erwarten ist.
7. Eine Nutzung von Kommunikationsdaten zu anderen Zwecken, beispielsweise durch Nachrichtendienste, durch sonstige Behörden oder durch private Dritte, ist auszuschließen. Den speichernden Diensteanbietern selbst ist die Nutzung der Daten nur insoweit zu gestatten, wie es zur Entgeltermittlung und Entgeltabrechnung erforderlich ist.
8. Der Zugriff auf und die Verwertung von Informationen über die Kommunikation von Ärzten, Rechtsanwälten, Steuerberatern, anderen Berufsgeheimnisträgern sowie Journalisten sind nur in besonderen Ausnahmefällen zuzulassen.
9. Zur Datenspeicherung und -vorhaltung sind nur Anbieter öffentlich zugänglicher Kommunikationsdienste und Betreiber öffentlicher Kommunikationsnetze zu verpflichten. Kleine Anbieter, insbesondere im Internetbereich, sind auszunehmen.
10. Die positiven und negativen Auswirkungen der Vorratsdatenspeicherung auf die Gesellschaft sind von einer unabhängigen Stelle zu untersuchen. Die Ergebnisse sind zu veröffentlichen. Der Bundesdatenschutzbeauftragte hat dem Deutschen Bundestag alle zwei Jahre Bericht über die Erfahrungen mit der praktischen Anwendung der Vorratsdatenspeicherung zu erstatten. Die Berichte sind zu veröffentlichen.

Unterzeichner:

- Chaos Computer Club
- Deutsche Vereinigung für Datenschutz e.V. (DVD)
- Deutscher Journalisten-Verband e.V. (DJV)
- Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung e.V. (FIfF)
- Grüne Jugend Bundesverband
- Netzwerk Neue Medien e.V. (NNM)
- no abuse in internet e.V. (naiin)
- STOP1984
- Verein zur Förderung des öffentlichen bewegten und unbewegten Datenverkehrs e.V. (FoeBuD)
- Verbraucherzentrale Bundesverband e.V. (vzbv)

Schnüffelchips: RFID-Industrie setzt auf PR-Offensive statt auf konstruktiven Dialog

Pressemitteilung von FoeBuD und DVD vom 18. Januar 2006

Am Donnerstag, den 19. Januar 2006, findet in den Räumen der Berlin-Brandenburgischen Akademie der Wissenschaften eine Lobby-Veranstaltung der RFID-Industrie statt. Veranstalter ist das »RFID-Informationsforum«, ein Zusammenschluss von Handel und Industrie. Durchgeführt wird sie von Pleon, einem der marktführenden PR-Unternehmen in Deutschland. Geladen sind ausschließlich Vertreter von Politik, Verbänden und Medien. KritikerInnen des RFID-Einsatzes – wie Datenschützer und Bürgerrechtler – sowie besorgte BürgerInnen bleiben außen vor.

»Mit immensem Kostenaufwand versucht die RFID-Industrie die Einführung dieser Kontroll- und Überwachungstechnik durchzudrücken. Gesprächsangebote wie das Expertenforum zu RFID beim Bundeswirtschaftsministerium werden dagegen von Industrie und Handel blockiert – Kritik soll offenbar mit PR erstickt werden«, bewertet Rena Tangens vom FoeBuD die Aktivität der RFID-Lobbyisten.

Die Bundesregierung hatte seit Sommer 2004 Handel, Datenschützer und Verbraucherschützer zu mehreren Treffen eines Expertenforums geladen, um gemeinsam die Rahmenbedingungen der Nutzung von RFID in Konsumgütern auszuloten. Für die DVD meint ihr Vorstandsvorsitzender Sönke Hilbrans: »Die Verbreitung von RFID in Konsumgütern als elektronischer Produktcode (der so genannte epc) birgt erhebliche Datenschutzprobleme, die für die BürgerInnen nicht beherrschbar sind.

Trotz intensiver Diskussionen im Expertenforum des Bundeswirtschaftsministeriums weigert sich die RFID-Lobby bis heute, anzuerkennen, dass RFID-Kennungen in Konsumgütern personenbezogene Daten sind. Wir fragen uns, ob die Industrie an einer Einigung mit Daten- und Verbraucherschützern überhaupt noch interessiert ist.«

Auch Rena Tangens vom FoeBuD ist unzufrieden mit dem bisherigen Verlauf der Gespräche: »Von Seiten der Industrie gibt es bisher noch nicht einmal eine ernstzunehmende Selbstverpflichtungserklärung zum Verbraucherschutz. Bei jedem Arbeitstreffen gibt es nur immer wieder aufgewärmte unverbindliche Absichtserklärungen. Offensichtlich nutzt die Industrie die Konsultationen nur, um Zeit zu gewinnen, inzwischen Politiker durch bezahlte Lobbyisten zu beeinflussen und durch RFID-Einsatz Fakten zu schaffen. Mit dieser Hinhaltetaktik versucht die RFID-Lobby zu verhindern, dass wirksame gesetzliche Regelungen für die RFID-Nutzung zum Schutz der Bürger erlassen werden. Wir lassen uns das nicht länger bieten.«

Auch für den Fall eines Ausstiegs aus den Konsultationen der Bundesregierung ist für die Bürgerrechtler die Frage der RFID-Chips nach wie vor aktuell: »Wir werden dann die gewonnene Zeit für mehr Öffentlichkeitsarbeit, Verbraucheraufklärung, Proteste und Demonstrationen nutzen«, so Tangens.

»Für einen konstruktiven Austausch sind wir aber nach wie vor offen.«

RFID (Radio Frequency IDentification) sind winzige Chips mit Antenne, die eine weltweit eindeutige Seriennummer enthalten und ohne Sichtkontakt aus einiger Entfernung und unbemerkt per Funk ausgelesen werden können. RFID-Chips sollen nach dem Willen von Handel und Industrie in Zukunft u.a. die Strichcodes auf den Waren ersetzen.

Anders als beim Strichcode, der das Produkt nur der Art nach bezeichnet, ist mit RFID jedes einzelne Hemd und jede einzelne Packung Frischkäse über die weltweit eindeutige Seriennummer identifizierbar und kann damit Personen zugeordnet werden. RFID-Chips bringen eine neue Dimension des Datensammelns, der Überwachung und Manipulation.

RFID-Chips betreffen Menschen deshalb nicht nur in ihrer Eigenschaft als Verbraucher, sondern sie können zu einer Gefahr für Bürgerrechte und Demokratie werden.

Weitere Infos: www.stoprfid.de

FoeBuD verkauft Schutzhülle gegen unbefugtes Auslesen von RFID-Ausweisen

Pressemitteilung des FoeBuD e.V. vom 7. Februar 2006

Die neuen Reisepässe der Bundesrepublik Deutschland sind mit einem RFID-Schnüffel-Chip zur drahtlosen Übertragung ausgestattet, auf dem relevante biometrische Daten gespeichert werden. Ein unbefugtes Auslesen durch Dritte ist nicht auszuschließen. Als wirksamer Schutz gegen diese Zugriffe wurde eine Schutzhülle entwickelt, die aus einer extrem dünnen Kunststoff/Metalllegierung besteht. Sie verhindert wirksam die Kommunikation des im ePass integrierten Chips mit der Außenwelt. Die im ePass gespeicherten Daten werden dabei keineswegs verändert oder gar zerstört. Wird der Reisepass aus der Schutzhülle entnommen, stehen alle Funktionen wieder uneingeschränkt zur Verfügung.

»Die Schutzhülle ist keine Lösung der Probleme mit der Schnüffelchiptechnik«, so padeluun vom FoeBuD e.V., »Aber man kann mit Ihr Diskussionen um das Thema anregen und so das abstrakte Thema veranschaulichen.« Richtige Lösungen müssten in einem Gremium erarbeitet werden, in dem nicht nur die Industrie, sondern auch Bürgerrechtler, Daten- und Verbraucherschützer miteinander an einer kontrollierten Einführung von RFID arbeiten. »Solange die Schnüffelchips zu Lasten der Sicherheit von Bürgerinnen und Bürgern eingeführt werden, müssen Sie sich wohl oder übel mit solchen Schutzhüllen helfen. Das Ziel ist es aber, dass solche Hilfsmittel nicht vonnöten sind« resümiert padeluun.

Die Schutzhülle ist für 6,00 Euro zuzüglich Versandkosten im FoeBuD-Shop (https://shop.foebud.org) erhältlich.

»Befreite Dokumente« für alle im Internet abrufbar

Gemeinsame Aktensammelstelle des FoeBuD e.V. und des CCC zum Informationsfreiheitsgesetz geht online – Presseerklärung vom 06.03.2006

Der Bielefelder FoeBuD e.V. hat gemeinsam mit dem Chaos Computer Club ein Internetportal eingerichtet. Bürgerinnen und Bürger können hier Akten einstellen und anderen zugänglich machen, die sie zuvor über das neue Informationsfreiheitsgesetz (IFG) angefordert haben. Damit können andere die hohe Gebühr (bis zu 500 Euro) für die Akteneinsicht sparen und die Behörden werden von doppelter Arbeit entlastet. Die gemeinsame Aktensammelstelle ist ab sofort unter http://www.befreite-dokumente.de zu erreichen.

»Wir möchten Bürgerinnen und Bürgern das Informationsfreiheitsgesetz schmackhaft machen und zeigen, dass es tatsächlich genutzt wird«, erläutert Mitinitiator Frank Rosengart vom Chaos Computer Club, »zudem kritisieren wir die hohen Gebühren und möchten die Behörden ermuntern, die Akten von sich aus zu veröffentlichen«.

Auf der Internetplattform können Bürgerinnen, Journalisten oder Anwälte sehr einfach die Akten der Öffentlichkeit zugänglich machen, die per IFG von den Behörden »freigekauft« wurden. So können die Kosten für eine Recherche minimiert werden und der Staat wird transparenter. Akten, die bereits digital vorliegen, können direkt eingespielt werden. Ansonsten gibt es auch eine Faxnummer (040-40180156), an die man Akten schicken kann. Auch der Postweg steht offen (FoeBuD e.V., Befreite Dokumente, Marktstraße 18, 33602 Bielefeld). Die Aktensammelstellte fungiert als »Marktplatz«, wo sich Interessierte finden können, um die Kosten für eine Anfrage zu teilen.

»Es ist eigentlich die Aufgabe der Behörden, eine solche Plattform bereit zu stellen, aber das wird noch einige Jahre dauern«, bedauert Axel Rüweler vom FoeBuD e.V. »Die hohen Gebühren kann sich kaum jemand leisten und stehen im krassen Gegensatz zu dem, was das Gesetz eigentlich bezwecken sollte. Mit dem Portal versuchen wir, den Gebühren ein wenig entgegenzuwirken. Der Gesetzgeber ist aufgefordert, hier für Abhilfe zu sorgen.«

Hintergrund: Das »Gesetz zur Regelung des Zugangs zu Informationen des Bundes« oder kurz Informationsfreiheitsgesetz (IFG) ist seit dem 1. Januar 2006 in Kraft. Das IFG regelt den Zugang zu Akten und Dokumenten und gibt jedem interessierten Bürger die Möglichkeit, beliebige Akten ohne Begründung anzufordern oder einzusehen, sofern nicht wichtige Gründe dagegen sprechen. In den Bundesländern Berlin, Brandenburg, Nordrhein-Westfalen und Schleswig-Holstein gibt es seit Jahren vergleichbare Gesetze. Das Auswärtige Amt war zuletzt in die Kritik geraten, weil es für vier Seiten Fotokopien 106 Euro an Gebühren verlangte.

»Internationale Liga für Menschenrechte« protestiert gegen geheimdienstliche Überwachung ihres Präsidenten

Presseerklärung der »Internationalen Liga für Menschenrechte« vom 21.02.2006

Der Vorstand der »Internationalen Liga für Menschenrechte« hat mit Empörung zur Kenntnis genommen, dass Liga-Präsident Dr. Rolf Gössner weiterhin unter geheimdienstlicher Beobachtung des Bundesamtes für Verfassungsschutz (BfV) steht. Das geht aus einem Dossier des Bundesamtes hervor. Die Liga protestiert aufs Schärfste gegen diese Ausforschung ihres Vorsitzenden durch den deutschen Inlandsgeheimdienst. Es bestehe die große Gefahr, dass damit auch eine international anerkannte Menschenrechtsvereinigung ins Visier des Verfassungsschutzes geraten ist und weiterhin gerät.

Rolf Gössner hat gegen die Bundesrepublik Deutschland Klage beim Verwaltungsgericht Köln erhoben und letzte Woche die Klagebegründung eingereicht. Die Klage ist zunächst auf eine vollständige Auskunft des BfV über alle zu seiner Person gespeicherten Daten gerichtet, da das Amt weitergehende Auskünfte wegen »Geheimhaltungsbedürftigkeit« und »Ausforschungsgefahr« sowie zum Schutz von »Quellen« verweigert hat; in einem weiteren Schritt soll die Rechtmäßigkeit der Erfassung gerichtlich überprüft und eine Löschung der Daten erstritten werden. Dieses Verfahren hat über den Einzelfall hinaus grundsätzliche Bedeutung, denn es geht um ein brisantes Problem, das auch andere Publizisten, Rechtsanwälte und Menschenrechtler betrifft: Welche Grenzen sind den kaum kontrollierbaren Nachrichtendiensten und ihren geheimen Aktivitäten gezogen – besonders im Umgang mit Berufsgeheimnisträgern und im Rahmen unabhängiger Menschenrechtsarbeit von Nichtregierungsorganisationen?

Zur Vorgeschichte: Voriges Jahr hat Rolf Gössner auf seinen Antrag vom BfV das vorerst letzte Dossier über seine ihm zur Last gelegten Aktivitäten erhalten. Grund für seine Überwachung ist laut BfV, dass er Kontakte zu Gruppen und Personen hat, die der Verfassungsschutz (VS) als »linksextremistisch« oder »linksextremistisch beeinflusst« einstuft, ohne jedoch Kriterien für diese Einstufung zu benennen. Dazu zählen etwa die »Vereinigung der Verfolgten des Naziregimes« (VVN) und die Rechtshilfegruppe »Rote Hilfe e.V.«. Bei den über Gössner gesammelten »Sünden« handelt es sich insbesondere um seine Artikel, Reden und Interviews, die in bestimmten Publikationen – etwa in den Tageszeitungen »Junge Welt« und »Neues Deutschland« – erschienen sind sowie um Lesungen und andere Veranstaltungen mit bestimmten Veranstaltern, wie etwa der VVN oder der »Rosa-Luxemburg-Stiftung«.

Letzten Endes wird Rolf Gössner eine Art »Kontaktschuld« zur Last gelegt, nicht etwa eigene verfassungswidrige Bestrebungen. Es handelt sich bei all diesen inkriminierten Beiträgen ausschließlich um Berufskontakte im Rahmen seiner vielfältigen beruflichen und ehrenamtlichen Tätigkeiten, insbesondere seiner Bürger- und Menschenrechtsarbeit. In zahlreichen Publikationen hat er sich kritisch u.a. mit den Praktiken der Sicherheitsorgane, besonders auch der Geheimdienste befasst, so etwa in seinem letzten Buch »Geheime Informanten. V-Leute des Verfassungsschutzes: Kriminelle im Dienst des Staates« (Knaur-Verlag, München 2003).

Immer wieder laden ihn Bundestag und Landtage als Sachverständigen ein, um in Gesetzgebungsverfahren u.a. Polizei- und Geheimdienst-Gesetzentwürfe zu begutachten. Auch von der Polizeiführungsakademie, von Polizeifachhochschulen und selbst vom Verfassungsschutz ist er als Experte zu Vorträgen und Diskussionen eingeladen worden.

Rolf Gössner ist für die Liga auch Mitherausgeber des jährlich erscheinenden »Grundrechte-Reports – Zur Lage der Bürger- und Menschenrechte in Deutschland« (Fischer-Verlag, Ffm) sowie Mitglied in der Jury zur Vergabe des Negativpreises »BigBrother-Award«, der an Institutionen und Personen verliehen wird, die besonders gegen Datenschutz und informationelle Selbstbestimmung verstoßen haben – so wie voriges Jahr an den ehemaligen Bundesinnenminister Otto Schily (SPD), auf den Gössner die »Laudatio« gehalten hat (dokumentiert in: Frankfurter Rundschau vom 31.10.2005). [...]

Der Verfassungsschutz beobachtet Rolf Gössner schon seit 1970, also seit nunmehr 35 Jahren. Kurz nach dem ersten Bekanntwerden vor zehn Jahren hatte diese Affäre erhebliche öffentliche Reaktionen hervorgerufen. Der Verband Deutscher Schriftsteller, die IG Medien, die Deutsche Journalisten-Union, Juristenorganisationen, acht Bürgerrechtsgruppen – darunter die Liga - sowie zahlreiche prominente Schriftsteller des deutschen P.E.N.-Zentrums haben sich seinerzeit in Offenen Briefen an das BfV gewandt und gegen die geheimdienstliche Erfassung ihres Kollegen protestiert; auch der Deutsche Bundestag und die Bundesregierung haben sich mit seinem Fall befasst – allerdings ohne Ergebnis. Die Beobachtung ging jedenfalls weiter, auch unter der rot-grünen Regierungskoalition, und dauert nachweislich bis heute an.

Die Maßnahmen dieser geheimdienstlichen Langzeitüberwachung eines engagierten Rechtsanwalts, Publizisten und Menschenrechtlers verletzen die Persönlichkeitsrechte, den Informantenschutz, das Mandatsgeheimnis und die ausforschungsfreie Sphäre, die für unabhängige Menschenrechtsgruppen unabdingbar ist.

Der Vorstand der Liga fordert das Bundesamt für Verfassungsschutz und die für den Inlandsgeheimdienst verantwortliche Bundesregierung auf, die Überwachung des Liga-Präsidenten Dr. Rolf Gössner unverzüglich einzustellen und ihm gegenüber sämtliche erfassten Daten offenzulegen!

Kontakt: Dr. Rolf Gössner (Bremen)
Tel. 0421/703354 rolf-goessner@ilmr.de



Ich bin der liebe Wolf